21世纪高职高专规划教材

计算机应用系列

Jisuanji Wangluoguanli Yu Anquan

赵立群 主编

车亚军 车东升 副主编

计算机网络管理与安全

清华大学出版社



21 世纪高职高专规划教材·计算机应用系列

计算机网络管理与安全

赵立群　主　编
车亚军　车东升　副主编

清华大学出版社
北　京

内容简介

计算机网络安全既是推进信息化的基础保障，也是信息系统正常运行的关键环节。本书针对高职高专的教学特点，坚持实用技术和实际案例相结合的原则，注重操作能力和实践技能的培养，以管理与安全为主线，介绍当前计算机网络管理与安全的主要技术与工具。内容包括：基于 Windows 2003 的活动目录管理方法、Windows 2003 网络服务功能 、SNMP 协议，以及加强计算机网络安全管理等技术应用。

本书的实用性和操作性并重，且充分考虑到高职学生的特点和社会需求，注重学生实践能力的培养。本书不仅适用于高职高专院校计算机、信息管理、电子商务、物流管理等各专业的教学；也可作为企业从业人员在职培训以及社会 IT 人士提高应用技能与技术的教材；对于广大自学者也是一本有益的读物。

图书在版编目(CIP)数据

计算机网络管理与安全/赵立群主编. —北京：清华大学出版社，2008. 10
21 世纪高职高专规划教材. 计算机应用系列
ISBN 978-7-302-17691-6

Ⅰ. 计…　Ⅱ. 赵…　Ⅲ. ①计算机网络—管理—高等学校：技术学校—教材 ②计算机网络—安全技术—高等学校：技术学校—教材　Ⅳ. TP393

中国版本图书馆 CIP 数据核字(2008)第 074141 号

责任编辑：田　梅
责任校对：袁　芳
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www. tup. com. cn　　**邮　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup. tsinghua. edu. cn
质　量　反　馈：010-62772015，zhiliang@tup. tsinghua. edu. cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　**印　张**：16. 5　　**字　数**：379 千字
版　次：2008 年 10 月第 1 版　　**印　次**：2008 年 10 月第1 次印刷
印　数：1～　000
定　价：　.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：023714-01

编 委 会

序言

PREFACE

微电子技术、计算机技术、网络技术、通信技术、多媒体技术等高新科技日新月异的飞速发展和普及应用，不仅有力地促进了各国经济发展，加速了全球经济一体化的进程，而且使当今世界迅速跨入到信息社会；以计算机为主导的计算机文化，正在深刻地影响着人类社会的经济发展与文明建设，以网络为基础的网络经济，正在全面地改变着人们传统的生活方式、工作方式和商务模式。

随着我国改革开放进程的加快，伴随着我国加入 WTO 以及我国市场经济体制的不断完善与发展，中国经济正在迅速融入世界经济，中国市场国际化的特征越来越明显。中国经济持续高速增长，进入到了一个最为活跃的经济发展时期。这一切都离不开高新科技的支持，都需要计算机、网络、通信、多媒体等现代化技术手段的支撑。为此，国家出台了一系列关于加强计算机应用和推动国民经济信息化进程的文件及规定，启动了电子商务、电子政务、金税等富有深刻意义的重大工程，加速推进“金融信息化、财税信息化、企业信息化和教育信息化”，全国掀起了新一轮的计算机学习与应用的热潮。

当今的时代处于网络化和信息化时代，很多工作都已经计算机化、网络化。随着我国国民经济信息化进程的加快，更加强调计算机应用与行业、企业的结合，更注重计算机应用与本职工作、具体业务的结合，计算机应用与本职工作结合的深度和广度已成为评价和考察一个人能否就业上岗、是否胜任本职工作的重要条件。目前，我国正处于改革与发展的关键时期，面对激烈的市场竞争和就业上岗的巨大压力，无论是即将毕业的各类学生还是下岗转岗的待业人员，努力学习计算机、熟练操作计算机、真正掌握好现代化科技工具，对于今后的发展都具有特殊意义。

针对我国高职教育“计算机应用”等信息技术应用专业知识老化、教材陈旧、重理论轻实践、缺乏实际操作技能训练等问题，为了适应我国国民经济信息化发展对计算机应用人才的需要，为了全面贯

彻教育部关于“加强职业教育”的精神和“强化实践实训、突出技能培养”的要求，根据企业用人与就业岗位的真实需要，结合高职高专院校“计算机应用”和“网络安全”等专业的教学计划及课程设置与调整的实际情况，我们组织北京联合大学、北方工业大学、北京财贸职业学院、首钢工学院、北方工业技术学院、北京石景山社区学院、北京城市学院、北京西城经济科学大学、北京朝阳社区学院、北京宣武社区学院、黑龙江工商大学等全国30多所高校及高职院校多年在一线从事计算机教学的主讲教师和具有丰富实践经验的企业人士共同撰写了这套教材。

本套教材包括：《计算机基础实例教程》、《微机组装（DIY）与维护》、《多媒体案例教程》、《办公自动化应用技术》、《Visual Basic. NET 基础教程》、《SQL Server 数据库案例教程》、《网页设计与制作实用教程》、《中小企业网站建设与管理》、《计算机网络管理与安全》、《管理信息系统》、《电子商务案例》11本书。在编写过程中，所有作者都自觉地以科学发展观为指导思想，严守统一的创新型格式化设计，采取任务制或项目制写法，贴近行业企业岗位实际，注重实用性技术与能力的训练培养，注重实践技能应用与工作背景紧密结合，同时也注重计算机、网络、通信、多媒体等现代化信息技术的新发展，使教材具有集成性、系统性、针对性、实用性、形式新颖和易于实施教学等特点。

本套教材不仅适合高职高专“计算机应用”和“网络安全”等专业及经济管理、税务、财会、金融类各专业学生的学历教育，同时也可作为广大工商流通企事业单位从业人员的职业教育和在职培训，对于其他自学者也是一本有益的读物。

系列教材编委会

2007年7月

前言

FOREWORD

随着计算机技术与网络通信技术的飞速发展，计算机网络应用已经渗透到社会经济领域的各个方面。计算机网络技术是现代信息科学与技术的重要组成部分，也是计算机管理信息系统的核心；计算机网络管理与安全既是信息化推进的基础保障，也是信息系统正常运行的关键环节，因而备受世界各国高度关注。

本教材针对计算机网络管理与安全等方面存在的管理及技术问题，按照教育部关于“加强职业教育、强化实践教学、突出技能和能力培养”教育教学改革精神，根据计算机网络管理与安全课程教学规律和特点，对原有的计算机网络管理、网络安全等内容进行了深度综合与提炼，并注意打通相关知识联系，采取了集成式写法。本书内容包括：基于 Windows 操作系统的活动目录管理方法、网络操作系统、网络管理、对因特网工作环境的支持、网络安全技术与应用、SNMP 协议管理等基本知识，以及加强计算机网络安全管理等技术应用。

全书共 8 章，采取新颖统一的格式化设计，突出案例教学，在案例的选择上具有实用性，以学习者应用能力培养与提高为主线，依照学习计算机网络管理与安全的基本过程和规律，以任务剖析的方式，结合知识要点循序渐进地进行讲解。本书在引导读者对知识和技术理解与掌握的基础上，通过多动手、多练习的方式，提高实践应用技能，注重动手能力的培养，以达到学以致用的目的。

目前，世界正处于科学技术的高速发展期，我国也正处在经济发展最活跃的时期，面对激烈的市场竞争，面对科技进步，所有企事业单位都在科学发展观的统领下加快信息化进程，加速信息技术应用，特别关注和加强计算机网络管理与安全的监控。当前面临企业拼发展，面临社会就业上岗的巨大压力，无论是企业员工、即将毕业的各类学生，还是下岗转岗的待业人员，努力学习和掌握计算机网络管理与安全的软件工具及技术应用，不断提高业务技术素质，对于今后的

发展都具有特殊意义。

本教材由李大军进行总体方案策划并具体组织，赵立群主编并统编全稿，车亚军和车东升为副主编，本书由具有丰富专业教学和企业实践经验的杜春涛教授审定。参加编写的人员有：车亚军（第 1 章），李多（第 2 章），王海珊（第 3 章），杨春（第 4 章），赵立群（第 5 章），孙钢凝（第 6 章），关忠（第 7 章），车东升（第 8 章）。

本书在编写过程中，广泛征集了各高等职业院校计算机网络管理与安全课程的主讲老师和有关企事业单位计算中心负责人对本书的修改意见与建议，得到了我国有关计算机行业协会的支持与帮助，得到了长期从事计算机教育教学有关专家教授的指导；在此，对参与本书出版论证与写作指导的牟惟仲、王纪平、张昌连、冀俊杰、吴明、林亚、储祥银、丁建忠、侯杰、沈煜、赵茜等同志一并表示衷心地感谢。由于时间紧，在编写过程中难免存在不足和疏漏，恳请各位专家及读者给予批评指正。

编　者

2007 年 7 月

目录

CONTENTS

第 1 章

基于操作系统的管理

【本章内容】

本章主要介绍网络操作系统的概念和工作模式，同时介绍在对等网模式下 Windows 2003 的组网过程，讲解 Windows 2003 提供的域模式与对等网模式各自的特点，使读者对基于操作系统的管理有一个初步认识。

【本章重点】

① 了解 Windows 2003 操作系统提供的网络工作模式。

② 掌握用 Windows 2003 在对等网模式下组网的方法。

③ 理解域模式中的基本概念和网络设计规划应注意的主要问题，掌握活动目录安装、卸载操作；理解网络操作系统的功能。

④ 了解网络操作系统在共享资源管理上的基本特点。

操作系统是用户与计算机之间的接口，是计算机系统资源的管理者，用户可以通过操作系统方便地使用计算机系统。本书第 1 章到第 3 章主要从应用层面上介绍以操作系统为工具对网络中的资源及用户进行管理的基本方法。

1.1　网络操作系统的主要功能和工作模式

网络操作系统（Network Operating System，NOS）是使网络上各计算机方便而有效地管理本地及网络资源，为网络用户提供所需的各种服务的系统软件。网络操作系统除了应具有操作系统的功能之外，还应提供高效、可靠的网络通信能力以及多种网络服务功能。

单机操作系统必须具备以下两个方面的功能：

(1) 为用户提供各种简便有效的访问本级资源的手段。

(2) 合理地组织系统工作流程，有效地管理系统。

为了实现以上两个基本功能，需要在操作系统中建立各种进程，编写不同的功能模块，并按层次结构的思想将功能模块组织起来，以完成处理器管理、存储管理、设备管理、

文件管理和作业管理等任务。

随着计算机网络技术的发展，各种规模的局域网纷纷被建立起来。传统的单机操作系统只能为本地用户使用本机资源提供服务，不能满足开放的网络环境的要求，对于联网的计算机系统，其资源既是本地资源，又是网络资源；既要为本地用户提供资源共享服务，又要为网络中的远程用户提供服务。网络操作系统的基本任务就是屏蔽本地资源与共享资源的差异，为用户提供各种基本的网络服务功能，完成网络共享系统的资源管理并提供网络系统的安全服务。

因此网络操作系统除了具有单机操作系统的功能外，还应具有以下功能：

（1）网络通信管理负责实现网络中计算机之间的通信。

（2）对网络中软硬件资源实施有效的管理，以保证用户方便、正确地使用这些资源，提高资源的利用率。

（3）提供网络访问的安全措施，保证系统中共享资源的安全性。

（4）提供网络服务，包括文件传输服务、打印服务、电子邮件服务等。

网络操作系统是网络的心脏和灵魂，是计算机网络不可缺少的系统软件，一个网络操作系统是一个复杂的计算机程序集合，它提供网络操作过程的协议或行为准则，没有网络操作系统，计算机网络就无法工作。一台计算机通过网络操作系统能访问同一网络的所有共享资源。

计算机网络在操作系统的干预下，有 3 种工作模式：对等网模式、工作站/服务器模式、客户机/服务器模式。

（1）对等网模式

网络中每台计算机的地位是平等的，既可以给其他计算机提供服务充当服务器，也可以向其他计算机索取服务充当客户机，网络中不存在明确的服务器和客户机。对等网模式如图 1-1 所示。

（2）工作站/服务器模式

网络以服务器为中心，严格地定义了每一个实体的工作角色，即网络上工作站无法在彼此之间进行文件传输，要通过服务器作为媒介，所有文件的读取、消息传送等是在服务器掌握之中。工作站/服务器模式如图 1-2 所示。

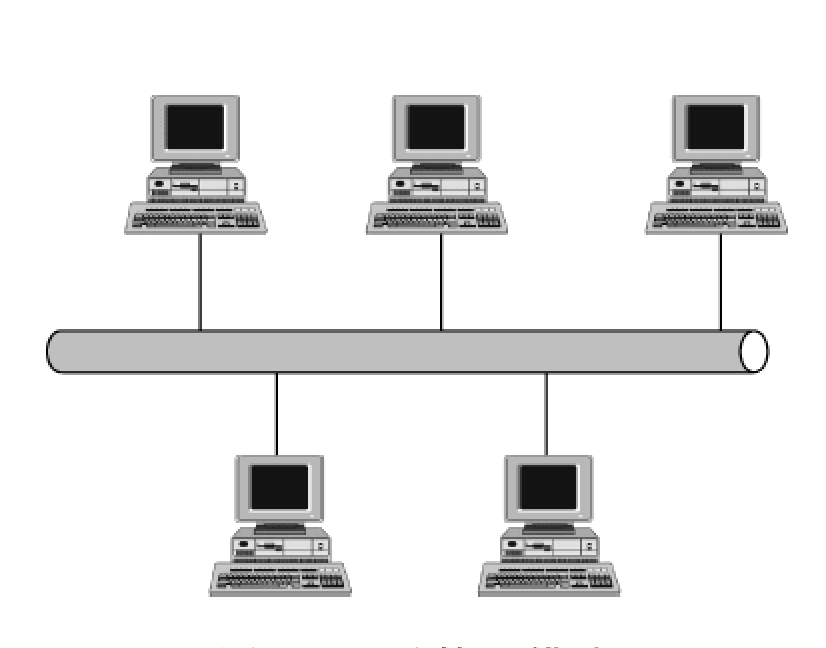


图 1-1　对等网模式

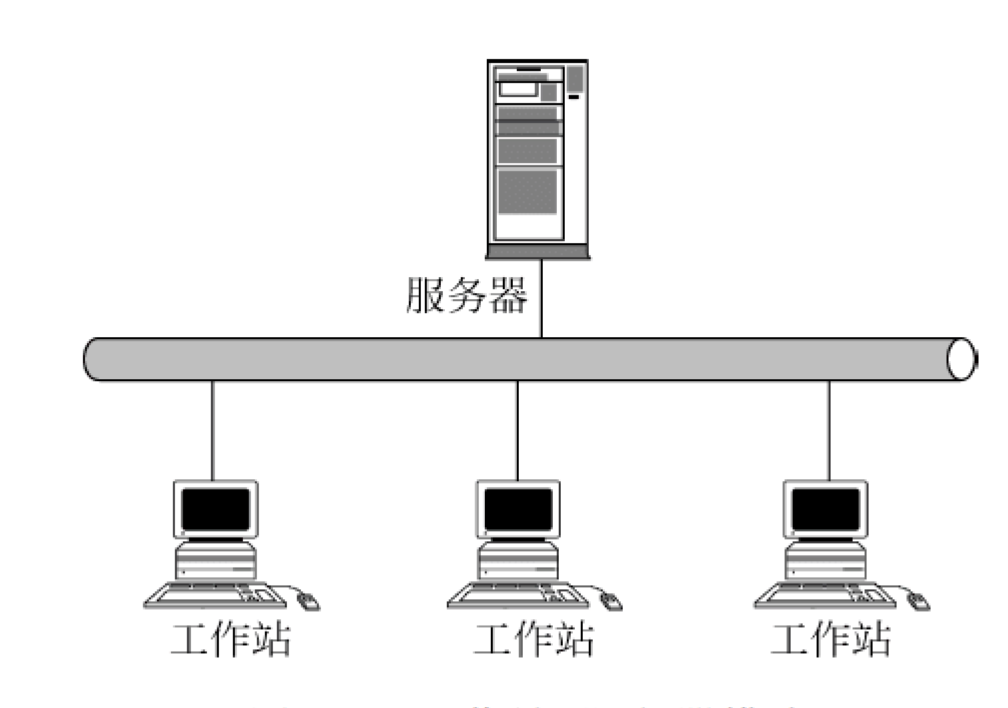
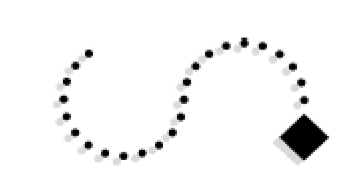
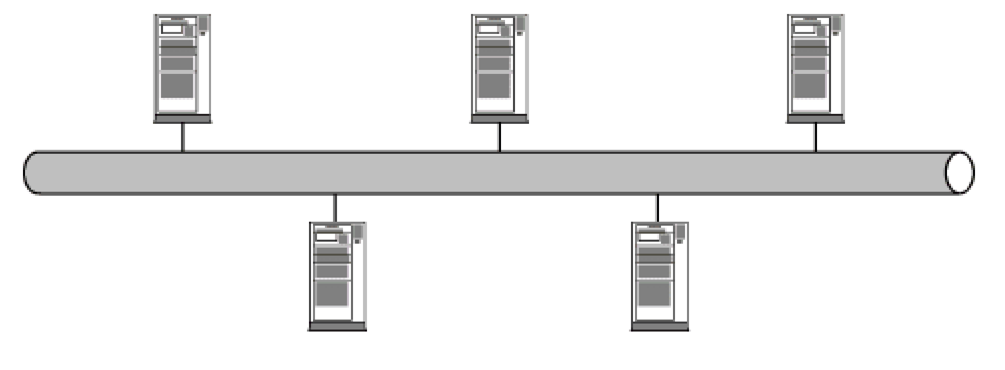


图 1-2　工作站/服务器模式



（3）客户机/服务器模式（主从模式）

由客户机、服务器上的各种服务程序构成的一种网络计算机环境，把应用程序要完成的任务分派到客户机和服务器上共同完成，其中的客户机和服务器并没有一定的严格界限，而取决于运行的软件。在客户机/服务器模式中，服务器所提供的不仅是文件、数据库功能，还有计算、通信等能力。工作时，由客户机和服务器各自负担部分计算或通信功能。客户机/服务器模式如图 1-3 所示。


图 1-3　客户机/服务器模式

3 种模式各自的优缺点，如表 1-1 所示。

表 1-1　3 种模式的比较

工作模式	优　点	缺　点
对等网	结构简单，资源直接共享，任何两台计算机可以直接通信	每台计算机以双重身份工作，负担重
	不需专用服务器	数据保密性差
		管理分散
工作站/服务器	可以按照不同的需要给予使用者相应的权限	多个使用者使用同一文件时，效率会降低
	文件安全管理较好	工作站资源不能直接共享
		一旦服务器有问题，将影响全网
客户机/服务器	任务由服务器、客户机分担，执行速度快。发生故障时，网络不会崩溃	管理较为复杂
	扩大系统时，容易加挂服务器或客户机	开发环境较为困难
	安全性好	

目前，网络操作系统并非只有一种，而是存在着多种操作系统。常见的有 Windows、Netware、UNIX 等。在这里只讲 Windows 2003，它的工作模式只有对等网和主从网两种。

1.2　对等网模式下的管理

Windows 2003 的对等网工作模式是以工作组方式来实现的，采用工作组组织方式的对等网具有以下特点：

- 工作组中的所有计算机之间是一种平等的关系；
- 工作组模式下资源和账户的管理是分散的；
- 每台计算机上有一套本地安全数据库，用来验证在本机登录的用户。

1.2.1　用户和组的管理

1. 用户的管理

在对等网模式中，采用本地用户账号的方式对用户进行管理。如果想使用某台计算机上的资源，就必须要在该计算机上有相应的账号，并且该账号对资源有一定的访问权

限。权限是与对象(通常是文件、文件夹或打印机)相关联的一种规则,它规定哪些用户可以访问该对象以及以何种方式访问。

用户账户包含了用户惟一的身份标识。在对等网模式下,可以创建本地用户账号。Windows Server 2003 还提供了内置的用户账户,用于协助用户进行日常的管理任务,或者临时访问资源。

(1) Administrator(管理员账户)

管理员账户具有对本机资源的完全控制权限,可以根据需要创建用户并指派相应的访问控制权限,该账户必须仅用于需要管理凭据的任务。由于大多数人都知道管理员这个账户,为了安全起见,可以将此账户设置为使用强密码或者重命名后赋予其最低的权限来进行保护。

(2) Guest(访客账户)

Guest 账户由在这台计算机上没有实际账户的用户使用。Guest 账户不需要密码。默认情况下,Guest 账户是禁用的,但也可以启用它。

可以设置 Guest 账户的权利和权限,设置方式与其他用户一样。默认情况下,Guest 账户是默认的 Guest 组的成员。默认情况下将禁用 Guest 账户,并且建议将其保持禁用状态。

2. 组的管理

如果多个用户对同一个资源有相同的访问权限时,逐个设置显然是非常愚蠢的事情,这时可以引入组的概念。组是用户账号的集合,可以将对网络资源中拥有相同的控制和访问权限的用户组织在一起,集中授权,统一管理。在对等网模式下,可以创建本地组。本地组是一种安全组,只被赋予了对创建该组的计算机上的资源进行访问的权利和权限。

关于对等网模式中用户和组的管理操作,将在 1.3 节的综合实训中作详细介绍。

1.2.2 共享资源的管理

在对等网中是通过对共享文件夹的设定来实现资源的共享。共享文件夹的设定方法非常简单,具体操作如下:

(1) 右击需要共享的文件夹,在出现的快捷菜单中选择“共享”命令,如图 1-4 所示。

(2) 在弹出的文件夹属性对话框中,选择“共享该文件夹”单选按钮,然后在“共享名”文本框中输入该共享文件夹的共享名称,如图 1-5 所示。

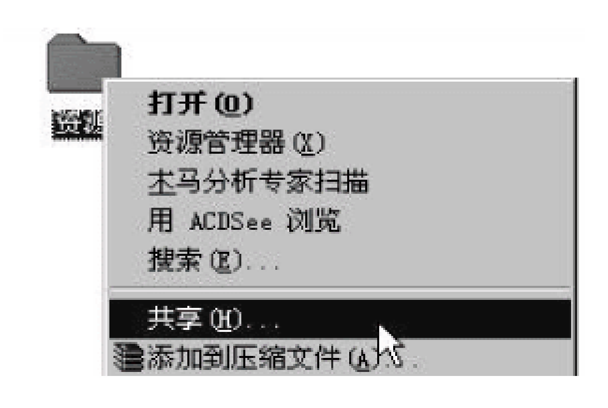


图 1-4 资源共享

(3) 默认情况下,系统对设置共享的文件夹都给 everyone 用户组完全控制的权限,当然这样做从安全角度考虑是非常不保险的,所以建议管理员根据情况适当改变权限。可通过单击“权限”按钮进行修改。

(4) 设置共享后,文件夹将会变成带有蓝色手形标志的共享文件夹图标。

不过要注意的是,在 Windows 2000/2003 系统中,有一种共享文件夹是在网上看不到的,那就是系统本身用于管理的共享文件夹,这类共享文件夹的共享名后面都带有一个“$”,如图 1-6 所示。



图 1-5　设置共享

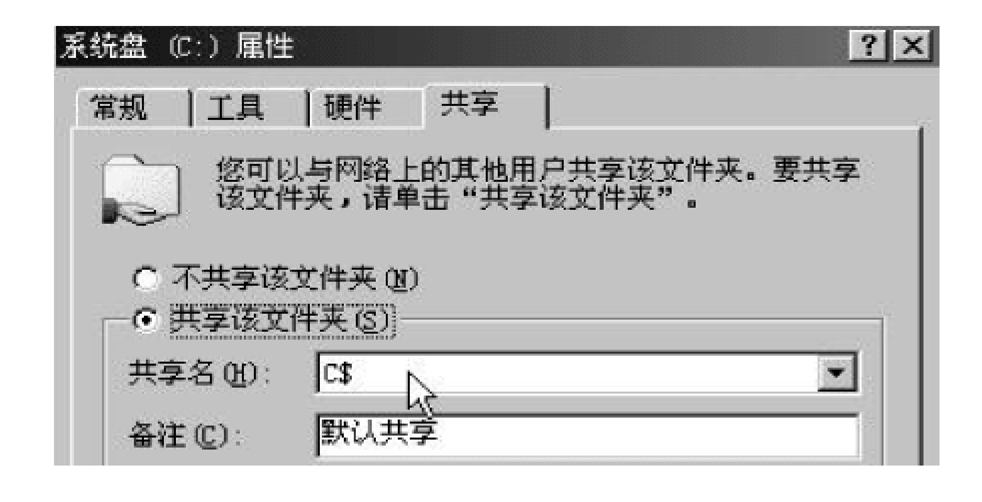


图 1-6　隐藏共享

这类共享文件夹通常是逻辑磁盘，这主要是出于安全和管理方面考虑的。用户虽然在“网上邻居”中看不到这类共享文件夹，但实际上该共享文件夹是存在的，用户输入“\计算机名\共享名 $”即可进入相应文件夹。

通过以上各步的配置，其他用户现在就可以通过“网上邻居”查看其他计算机上的共享资源了。在“网上邻居”中双击“选择邻近的计算机”选项即可显示对等网中所有计算机。要查看某计算机的共享资源，只需双击相应计算机名称即可。

1.3　综合实训

实训目的：

(1) 通过本实训理解工作组模式的特点。

(2) 通过本实训学会在工作组环境下进行资源的共享访问。

实训案例：

计算机 A 上 C 盘根目录有一个“教务处”文件夹，里面存储有一些供其他用户访问的文件。现要建立一个用户组“教务处组”，使得该组中的用户可以对“教务处”文件夹完全控制。计算机 B 的 C 盘上有“管理系”文件夹，要求建立一个“管理系组”的用户组，使得该组可以对“管理系”文件夹有完全控制权限。计算机 C 中建立一个用户名为 user3，密码为 abc123，要求用户 user3 可以通过计算机 C 访问计算机 A 上共享文件夹“教务处”及计算机 B 上共享文件夹“管理系”。

假设：计算机 A、B 的操作系统为 Windows Server 2003，计算机 C 的操作系统为 Windows XP 专业版。

1. 计算机 A、B、C 的共享资源设置

(1) 在计算机 A 上选择“开始”→“所有程序”→“管理工具”→“计算机管理”命令，如图 1-7 所示。



图 1-7　打开“计算机管理”窗口

（2）在弹出的“计算机管理”窗口左侧，右击“本地用户和组”下的“组”文件夹，在弹出的快捷菜单中选择“新建组”命令，如图 1-8 所示。

（3）在出现的“新建组”对话框中，在“组名”文本框中输入“教务处组”，单击“创建”按钮，如图 1-9 所示。



图 1-8　新建组



图 1-9　建立“教务处组”

（4）在“计算机管理”窗口右边的列表框中就出现新建的“教务处组”，如图 1-10 所示。

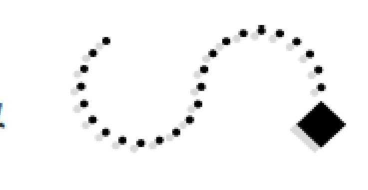




图 1-10　新建的“教务处组”

(5) 在“计算机管理”窗口左侧右击“用户”文件夹，在弹出的快捷菜单中选择“新用户”命令，如图 1-11 所示。

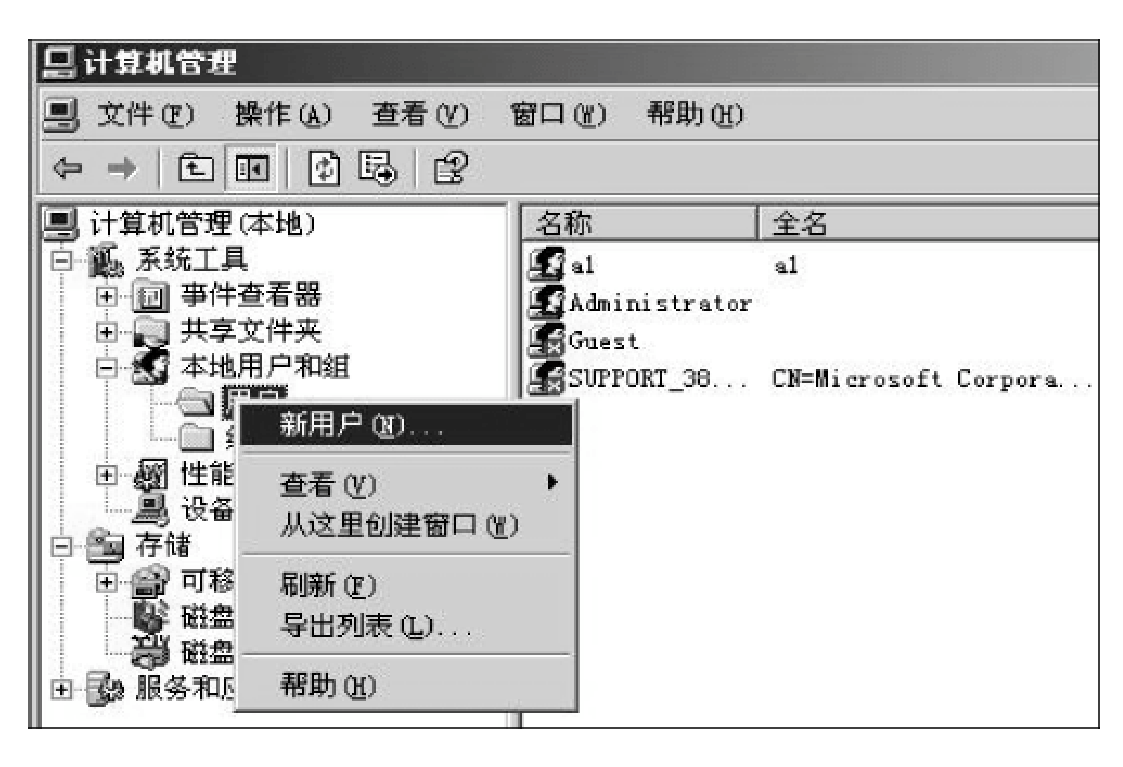


图 1-11　新建用户

(6) 出现“新用户”对话框。在“用户名”文本框中输入 user3，在“密码”文本框中输入 abc123，单击“创建”按钮，创建一个名为 user3 的新用户，如图 1-12 所示。

(7) 在“计算机管理”窗口中，右击 user3 用户。在弹出的快捷菜单中选择“属性”命令，如图 1-13 所示，弹出“user3 属性”对话框，如图 1-14 所示。

(8) 在“user3 属性”对话框中，单击“隶属于”选项卡，单击“添加”按钮，如图 1-15 所示。



图 1-12　“新用户”对话框



图 1-13　修改用户属性



图 1-14　“user3 属性”对话框

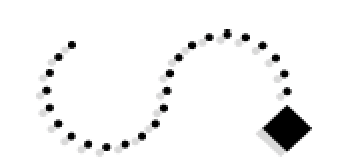


图 1-15　“隶属于”选项卡

(9)出现“选择组”对话框。在“输入对象名称来选择(示例)”文本框中输入“教务处组”,单击“确定”按钮,如图 1-16 所示。



图 1-16　“选择组”对话框



(10) 打开计算机 A 的“资源管理器”窗口，右击 C 盘下“教务处”文件夹，在弹出的快捷菜单中选择“共享和安全”命令，如图 1-17 所示，弹出“教务处 属性”对话框，如图 1-18 所示。

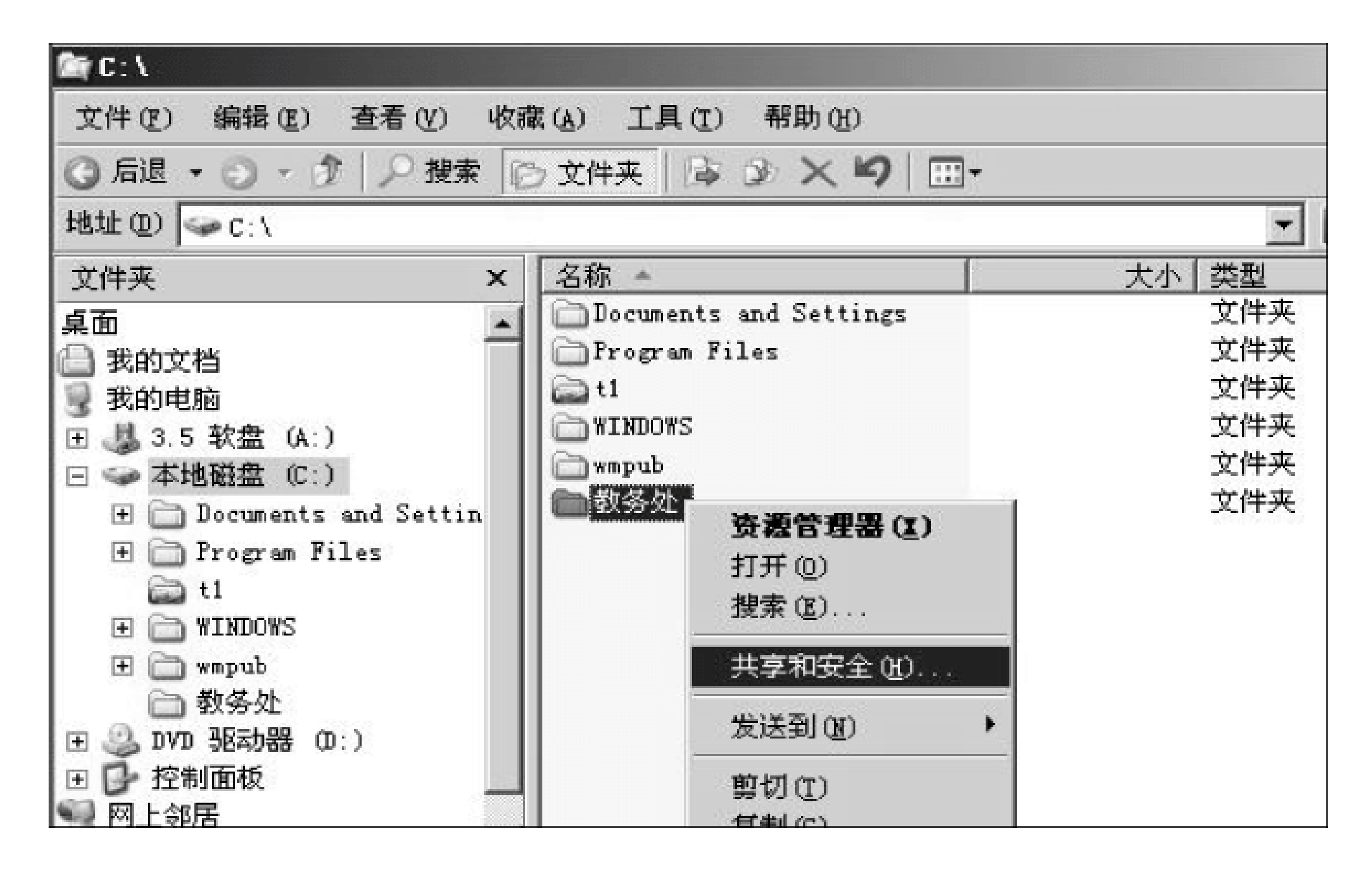


图 1-17　计算机 A 的资源管理器

(11) 在“教务处 属性”对话框中，选中“共享该文件夹”单选按钮，设置共享权限；在“共享名”文本框中输入“教务处”，如图 1-19 所示。

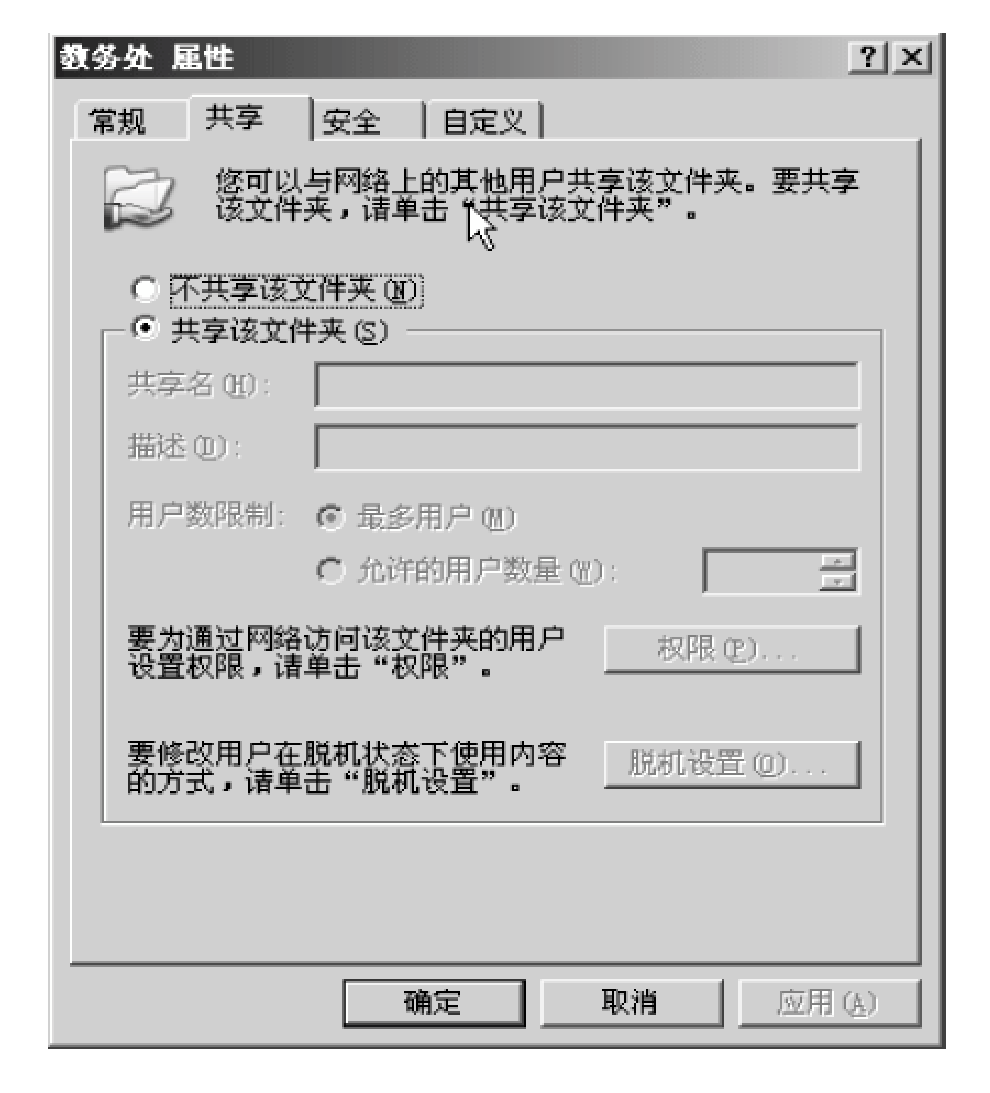


图 1-18　“教务处 属性”对话框



图 1-19　“教务处 属性”对话框

注意：共享名称可以和文件夹名称不同。

“用户数限制”选项组有两个单选按钮。

① “最多用户”：系统共享不限制用户的数量。

② “允许的用户数量”：可以在文本框中输入限制同时访问的用户数量，当超过这个

限制数目时，新用户将不能再访问该共享文件夹，只有等已经连接的用户断掉连接后，才能访问该共享文件夹。

(12) 在图 1-19 中单击“权限”按钮，出现“教务处的权限”对话框。单击“添加”按钮，添加新的组账号“教务处组”，如图 1-20 所示。

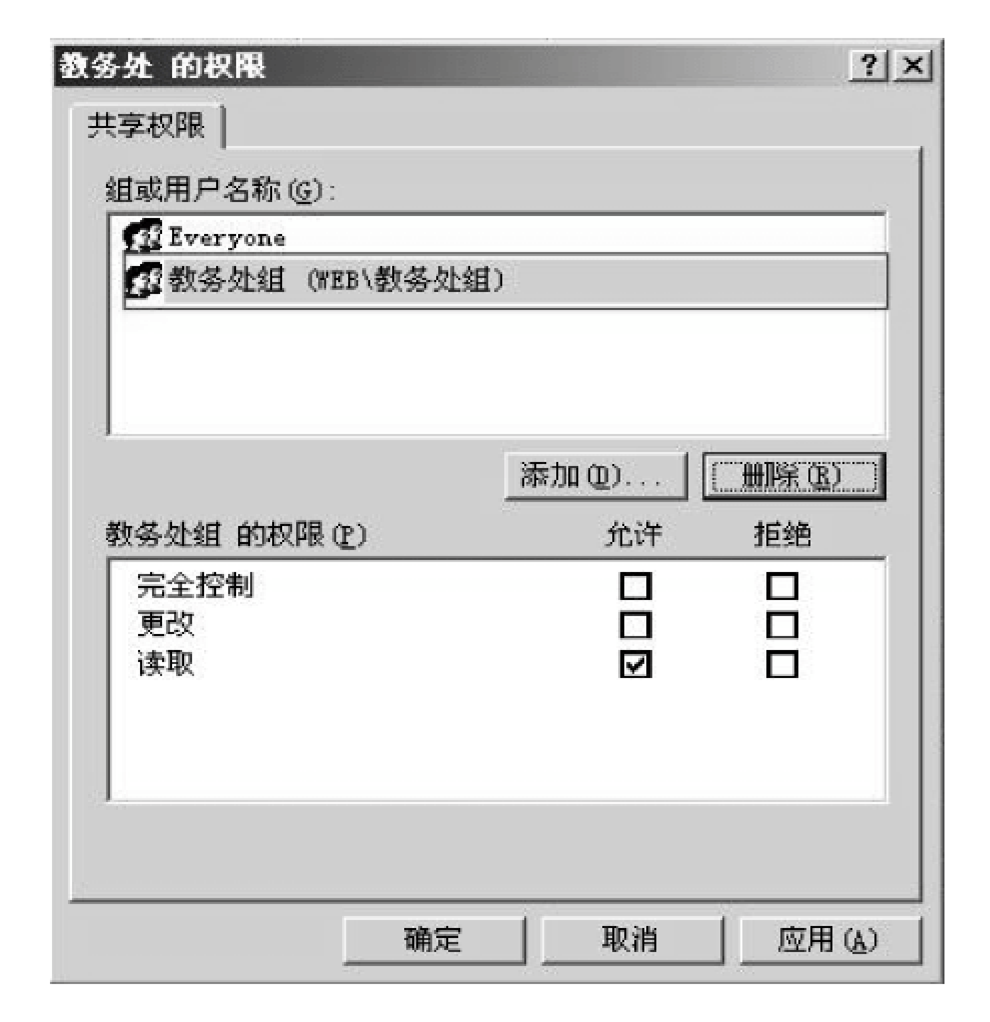


图 1-20 “教务处的权限”对话框

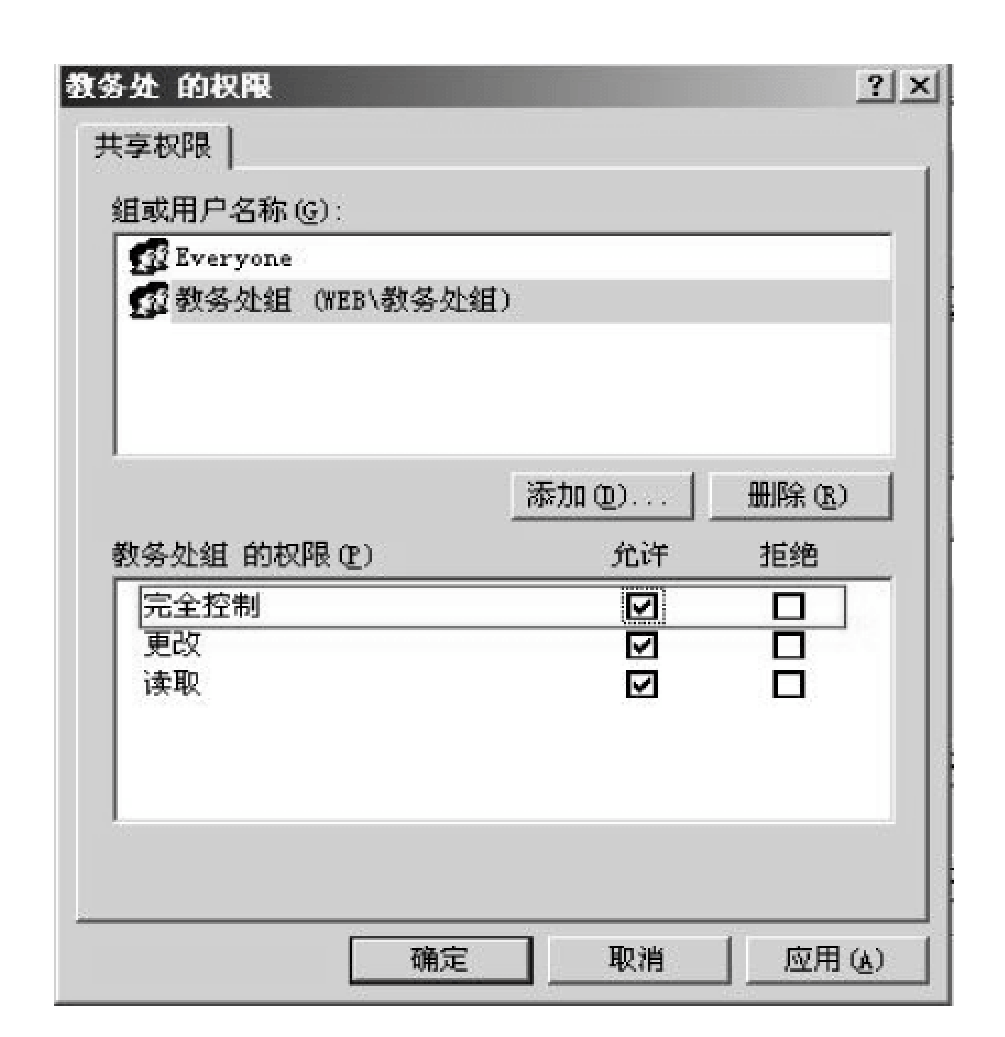


图 1-21 设置文件夹权限

(13) 在“组或用户名称”列表框中选择“教务处组(WEB\教务处组)”，然后在“教务处组的权限”列表框中选择“完全控制”权限，如图 1-21 所示，单击“确定”按钮，回到“教务处的权限”对话框。

(14) 单击“安全”选项卡，添加“教务处组”，如图 1-22 所示。

(15) 将“教务处组”的权限设置为“完全控制”，单击“确定”按钮，完成设置。

说明：在“共享”选项卡中设置的权限为“共享权限”，在“安全”选项卡中设置的权限为本地权限。如果从远程计算机进行访问，必须是两种权限的叠加。

(16) 在计算机 B 中按照上述步骤再创建一个“管理系组”，如图 1-23 所示。

(17) 在计算机 B 中同样创建一个新用户 user3，密码为 abc123，将该用户设置归属于“管理系组”，步骤同上面的操作，这里就不重复了。

(18) 打开计算机 B 中的“资源管理器”窗口，右击 C 盘下“管理系”文件夹，在弹出的快



图 1-22 设置文件夹访问权限

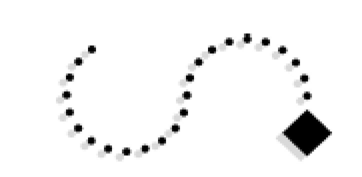




图 1-23　新建“管理系组”

捷菜单中选择“共享和安全”命令，如图 1-24 所示。按照上述步骤，设置“管理系组”对“管理系”文件夹的访问权限为“完全控制”。

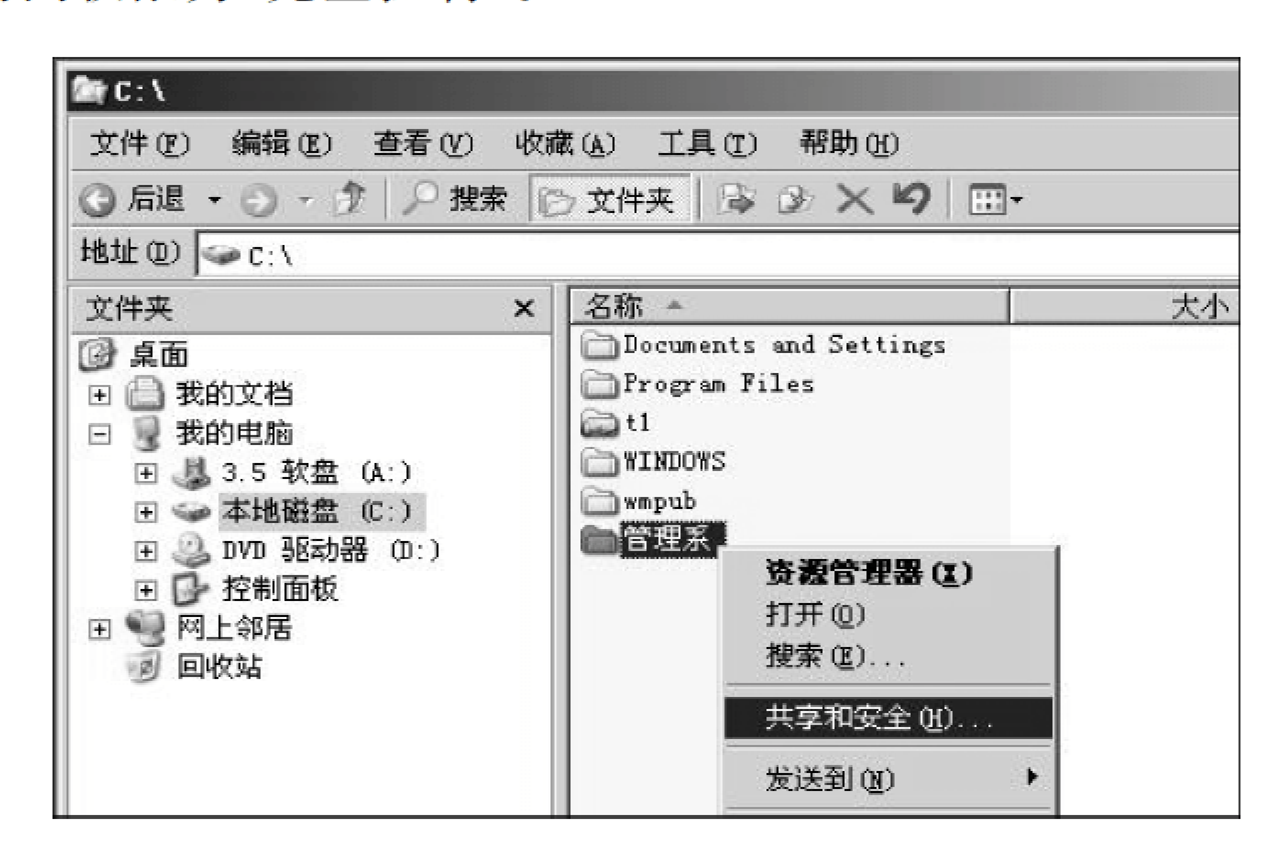


图 1-24　计算机 B 的资源管理器

(19) 在计算机 C 上，选择“开始”→“控制面板”→“管理工具”→“计算机管理”命令，建立用户 user3，设置密码为 abc123，如图 1-25 所示。



图 1-25　建立新用户

2. 访问共享资源

至此,准备工作已经就绪,下面开始实现如何在计算机 C 上访问计算机 A、B 上的资源。

方法 1:在“运行”对话框中输入“\IP 地址\共享名”进行访问。

方法 2:通过“网络邻居”进行访问。

提示:通过“网络邻居”进行访问,有时候在“网络邻居”中没有显示出要访问计算机的图标,这属于正常情况。“网络邻居”不能保证 100% 能访问,这里涉及了浏览服务,浏览服务的知识可以参考微软网站的网络广播课程。

http://www.microsoft.com/china/technet/webcasts/ondemand/episode.aspx?newsID=msft031105vxpm。

下面以方法 1 为例,介绍在计算机 C 上访问计算机 A“教务处”共享文件夹资源的操作步骤(计算机 A 的 IP 为 192.168.8.33)。

(1) 选择“开始”→“运行”命令,如图 1-26 所示,打开“运行”对话框。

(2) 在“打开”文本框中输入“\192.168.8.33\教务处”,192.168.8.33 为计算机 A 的 IP 地址,如图 1-27 所示。

(3) 单击“确定”按钮,弹出一个身份验证对话框。输入用户名 user3 和密码 abc123,单击“确定”按钮,系统会把输入的用户名、密码与计算机 A 存储的 user3 用户密码进行比对。密码一致则允许访问,不相同则拒绝访问,如图 1-28 所示。

(4) 验证合格后,进入计算机 A 中的“教务处”文件夹,如图 1-29 所示。

(5) 用户可以根据计算机 A 设置的权限进行相应的操作。本例中,user3 用户拥有对“教务处”文件夹的完全控制权限,因此可以创建一个名为“网络安全.txt”新文本文件,如图 1-30 所示。



图 1-26 “开始”菜单



图 1-27 “运行”对话框



图 1-28 计算机 A 密码确认对话框

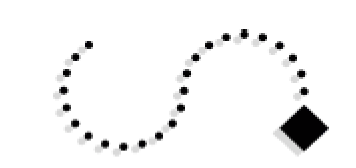




图 1-29　访问文件夹

下面以方法 2(“网络邻居”方法)为例,介绍在计算机 C 上访问计算机 B 中“管理系”共享文件夹资源。操作步骤如下:

(1) 在计算机 C 的桌面中双击“网上邻居”图标,如图 1-31 所示,弹出“网上邻居”对话框。



图 1-30　创建新文件



图 1-31　“网上邻居”图标

(2) 在 Workgroup 窗口右侧,显示了“网上邻居”中所有的计算机图标。双击计算机 B 的机器名 Web 图标(注:Web 是计算机 B 的机器名),如图 1-32 所示。



图 1-32　Workgroup 窗口

（3）在弹出的身份验证对话框中，输入用户名 user3 和密码 abc123，单击“确定”按钮，系统会把输入的用户名、密码与计算机 B 存储的 user3 用户密码进行比对，如图 1-33 所示。一致则可登录，否则无法进入计算机 B。



图 1-33　计算机 B 密码确认对话框

（4）在计算机 B 的共享资源窗口，双击“管理系”图标，如图 1-34 所示，打开“管理系”文件夹。

（5）本例中 user3 用户拥有对“管理系”文件夹的完全控制权限，可以右击“管理系”文件夹下的“linux 管理.txt”文件，在弹出的快捷菜单中选择“删除”命令，如图 1-35 所示，删除该文件后的窗口如图 1-36 所示。



图 1-34　“管理系”共享文件夹

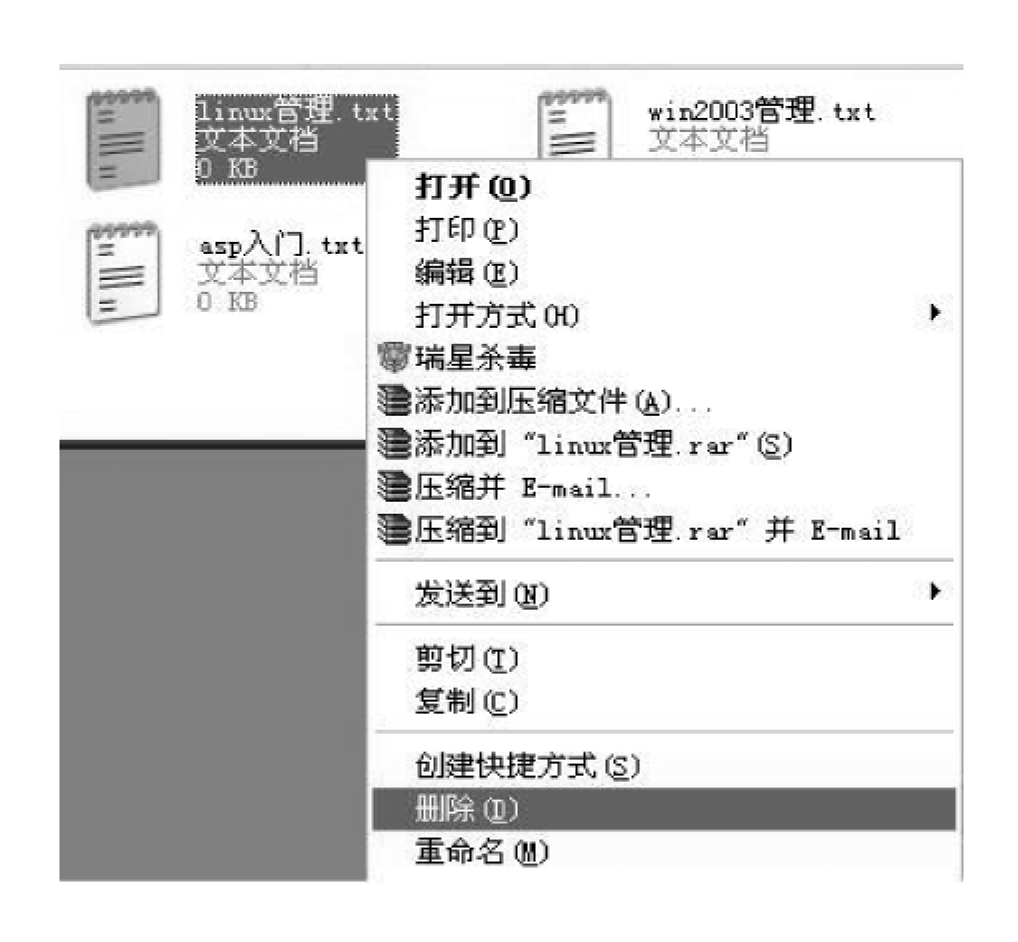


图 1-35　删除文件

说明：本例中，计算机 A 上“教务处”和计算机 B 上“管理系”文件夹如果直接给用户 user3 赋权，则步骤更少，但建议还是对组进行赋权，再把 user3 用户加到这个组中，这样

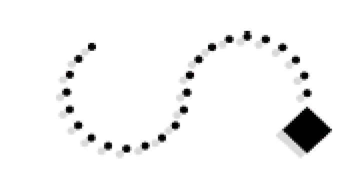




图 1-36　删除文件后的窗口

做是为了让大家养成良好的赋权习惯。如果用户增加，就会体现给组赋权的方便性。

小结：通过这个实训可以看出，在工作组模式中，由于账户分别存储在不同的计算机上，用户要访问网络中的其他计算机资源的时候，必须先要在其他计算机上建立其用户账户。随着网络规模的增大，这种工作组模式不灵活，效率比较低。建议网络规模比较大的情况下，要使用域的模式。

1.4　活动目录的基本概念

Windows 2003 的主从工作模式就是域工作模式，它是在 Windows 2003 提供的活动目录基础上运行的。若想管理和使用域模式下的网络，就应当很好地理解活动目录的工作方式、结构特点及其中一些基本概念。

1.4.1　域的概念

1. 什么是域

在对等网模式中，是以工作组方式来实现网络中各计算机之间的通信。工作组可以算是一种比较松散的组织，组中成员的加入和退出以及组中各台计算机中资源的管理都没有统一的要求，安全方面也没有保障。

那么在服务器中如何进行资源的集中管理和安全的保障呢？微软早在 Windows NT 时就提出了域的概念。域可以看成是一个带有安全边界的区域，在这个区域中的资源只对有资格进入区域的用户开放。

将域比作一个五星级宾馆，进入宾馆的顾客都要登记身份交付押金，然后得到一个房间的房卡。顾客手中的房卡(用户账号)只能打开指定的房间(域内的资源)，只有特定身份的人员才有能打开所有房间的钥匙。

域是一个具有集中安全控制机制的网络。在网络中选择一台计算机负责集中安全控制，这台计算机就成为域控制器，所有的计算机都共享域控制器上的账号和安全数据，无需各自建立本地账号，这种集权管理结构就叫做域。域比工作组能更有效地提高网络管理效率。

2. 域内计算机类型

域中计算机按照功能分为 3 种类型。

(1) 域控制器(Domain Controller)

域控制器专门负责管理域内用户账号和计算机安全。在网络中选择一台性能较好的计算机安装 Windows Server 2003,并起用活动目录(Active Directory,AD)服务,则该计算机就成为域控制器。域控制器管理用户域的交互,其中包括用户登录过程、身份验证和目录搜索。

(2) 成员服务器(Member Server)

安装了 Windows Server 2003 但没有起用活动目录的计算机,可以提供多种不同的网络服务,如 DHCP、DNS、IIS、FTP 等,这些计算机就成为成员服务器。成员服务器根据其提供的服务功能被冠以不同的名字,如文件服务器、数据库服务器、Web 服务器、DNS 服务器等。成员服务器不处理账号登录,不参与活动目录复制,也不存储域安全策略信息。成员服务器受域控制器的管理。

(3) 客户机

所有安装了 Windows 2000 Professional 或者 Windows XP,并且加入了域的计算机都是客户机。用户通过客户机访问域中的各种资源,执行应用程序。加入域的客户机都由域控制器负责用户身份的验证,并接受域控制器的管理。

安装 Windows 95/98 操作系统的计算机可以连接到域。用户可以从 Windows 95/98 系统的计算机登录到域,并访问域的资源,但这些计算机在域中没有计算机账号。

3. 域树和域林

单域可以满足一般中小企业的需求。对于大型企业以及有复杂需求的情况,可以通过多重域结构来实现。多重域结构有域树和域林两种结构。

(1) 域树

在 DNS 中,域树是指用来索引域名的反向分层树木结构。域树在目的和概念上与磁盘存储中计算机文件归档系统所使用的目录树很类似。例如,当磁盘上存储很多文件时,可以用目录将文件组织成逻辑集合,当域树有一个或者多个分支时,每一个分支都可以将名称空间中使用的域名组合成逻辑的集合。共用连续名称空间的域就组成一个域目录树。

在 Active Directory 中,域树是指一个或者多个域的层次结构,通过可传递的双向信任实现连接,从而形成一个连续的名称空间,多个域树也可以属于一个林。

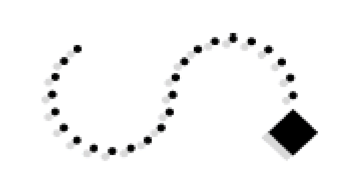
域树中的第一个域称为根域,相同域树中的其他域称为子域。域树的层次关系直接表现在域的命名方式上。每个下级域都继承了上一级域名。例如,某高校(Hqdx. com)下面有教学(Jiaoxue. hqdx. com)和培训(Peixun. hqdx. com)两个部门,其中教学部下有管理和外语两个系,培训下面有招生部,那么就可以通过建立域树来描述此结构,如图 1-37 所示。

注意:域树中的域只是在命名方式上有层次关系,在管理权限上是独立的管理个体。

(2) 域林

一片树林自然是由多棵树组成的,同样,目录林也是由多个目录树组成的。目录林中的域并不共用连续的名称空间。

当一个企业中有很多的公司,每个公司都有自己的域名系统时,就不能把这些有着完全不同域名系统的域放在一个域树中。我们可以采用域林解决这个问题。



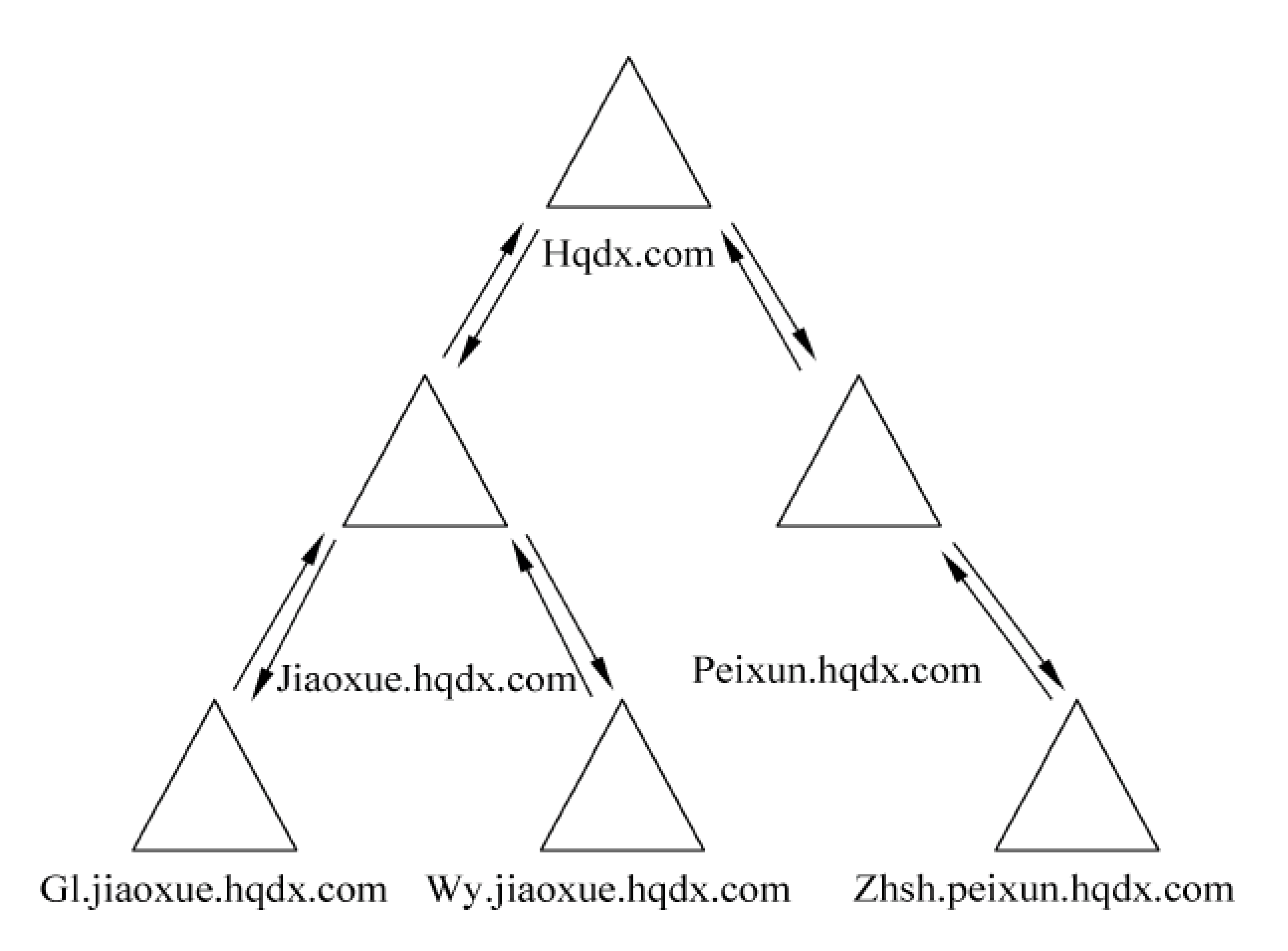


图 1-37　域树

比如，在北京的一个 A 公司，域名为 A. com，其下属 2 个子公司，域名为 Sale. A. com 和 Product. A. com；在上海有一个 B 企业，根域为 B. com，其下属 2 个子公司，域名为 Sale. B. com 和 Product. B. com。现在北京的 A 公司收购了上海的 B 企业，但 B 公司有一定品牌优势，在社会上有一定影响，所以合并后，不想改变 B 公司的域名，则可以采用域林的方法。这些 Active Directory 域本身的结构不相同，名称也不相同，如图 1-38 所示。

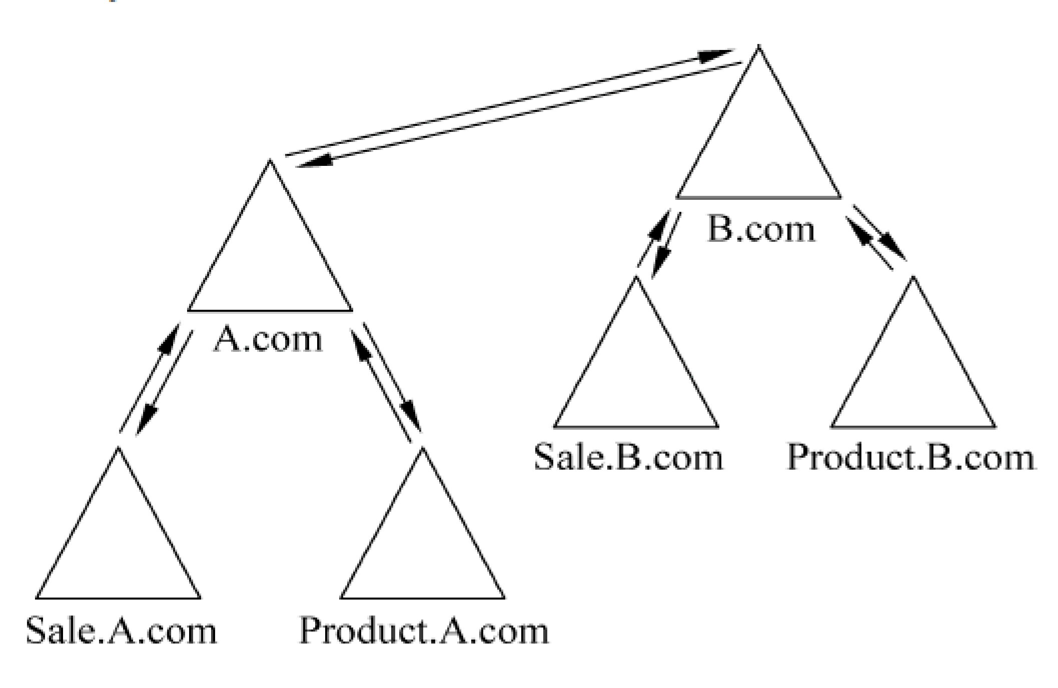


图 1-38　域林

1.4.2　组织单元的概念

域是一个带有安全边界的区域，在这个区域中有许多的资源和用户，为了方便对这些资源和用户的管理，需要将资源和用户进行归类，同一类的放在一起。组织单元(Organizational Unit，OU)便是引入的一个逻辑单位，它好比一个容器，将各种对象，如用户、组、计算机和其他组织单位放入其中。由于 OU 层次结构局限于域的内部，所以一个域中的 OU 层次结构与另一个域中的 OU 层次结构完全独立。

组织单元具有继承性，子单元能够继续父单元的访问许可权。每一个组织单元可以有自己单独的管理员并指定其管理权限，他们管理着不同的任务，从而实现了对资源和用

户的分级管理。组织单位是可以指派组策略设置或委派管理权限的最小作用域或单元。用户可在组织单位中的代表逻辑层次结构的域中创建容器,这样用户就可以根据组织模型管理账户,进行资源的配置和使用。有关组策略设置的详细信息,请参见第 2 章。

域 A. com 中,有很多用户,用户可以根据部门设置不同的组织单元(OU),如销售部门 OU、生产部门 OU、财务部门 OU,如图 1-39 所示。把用户放到这些不同的组织单元中,就可以集中地委派管理权限和指派策略设置。

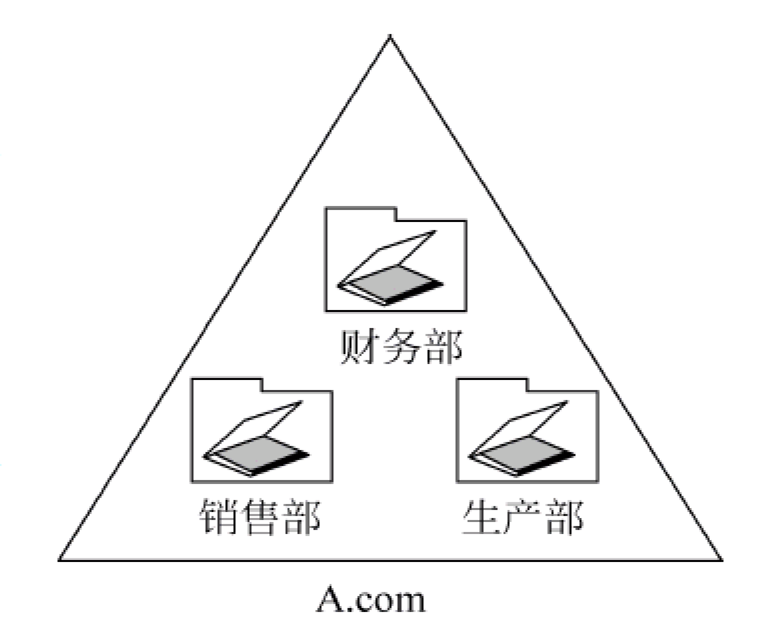


图 1-39　组织单元

1.4.3　组的概念

简单地说,可以将组看作是一个逻辑单位,它包含了一个或者多个用户账户,也可以包含其他的组。管理员将对每个资源的访问权限指派给这个组,而不是直接指派给具体的用户,那么,任何加入这个组中的账户或者其他组,也都具有了该资源的访问权限。组是可包含用户、计算机和其他组的活动目录或本机对象。使用组可以控制和管理用户和计算机对活动目录对象及其属性、网络共享位置、文件、目录、打印机等共享资源的访问,还可以向一组用户发送电子邮件。

下面介绍 Windows Server 2003 中的组的类型和作用域。

(1) 组的类型

在 Active Directory 中有两种类型的组:通讯组和安全组。可以使用通讯组创建电子邮件通讯组列表,使用安全组给共享资源指派权限。

安全组是可以列在随机访问控制列表(DACL)中的组,DACL 列表用于定义对资源和对象的权限。安全组也可以用于电子邮件实体,给这种组发送电子邮件,会将邮件发给组中的所有成员。

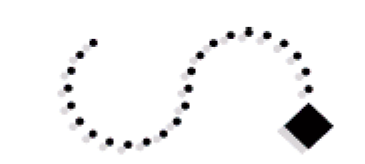
通讯组是只用于发送电子邮件并且没有启用安全性的组。不能将通讯组列在用于定义资源和对象权限的随机访问控制列表中。通讯组只能与电子邮件程序(如 Exchange Server)一起使用,以便将电子邮件发送到用户集合。如果需要组来控制对共享资源的访问,则创建安全组。

安全组提供了一种有效的方式来指派对网络上资源的访问权。使用安全组,可以将用户权限分配到 Active Directory 中的安全组,也可以对安全组指派用户权利以确定该组的哪些成员可在域内工作。

在安装 Active Directory 时,系统会自动将用户权限分配给某些安全组,以帮助管理员定义域中人员的管理角色。例如,在 Active Directory 中被添加到 Backup Operators 组的用户能够备份和还原域中每个域控制器上的文件和文件夹。在默认情况下,系统将备份文件和目录以及还原文件和目录的用户权利自动指派给 Backup Operators 组,因此该组的用户继承了指派给该组的用户权利。

(2) 组的作用域

组(不论是安全组还是通讯组)都有一个作用域,用来确定在域中该组的应用范围。



Windows Server 2003 的活动目录中有 3 类不同的组作用域：通用、全局和本地域。

本地域组。本地域组的成员包括 Windows Server 2003 域中的其他组和账户。本地组是面向资源的，管理员将网络访问权限赋予本地组，凡是加入到该本地组的所有成员的用户账户或者其他组就具有该本地组的资源访问权限。

全局组。全局组是面向用户账户的，用来组织具有相同权限的用户账户。通常把同一个部门的用户账户添加到一个全局组中。全局组的成员可以是用户账户或者是其他的全局组。全局组可在本域和有信任关系的其他域中使用，体现的是全局性。微软公司建议基于组织结构和行政结构进行规划。

通用组。通用组成员可包括域树或林中任何域中的其他组和账户，而且可在该域树或林中的任何域中指派权限。简单地说，通用组是用来管理、组织多个域的用户的。通用组一般用于多域的情况，通用组的成员信息保存在 DC 中。尽量避免通用组直接包含用户账号成员，可以使用全局组作为通用组的成员。

例如，在服务器上有一个名为“教务处”的文件夹，需要设置其访问权限。该文件夹中有用户 user1，user2，user3，其中 user1 属于域本地组“教师组”，user2 和 user3 属于全局组“艺术系组”。在设置权限的时候，尽量针对组进行赋权，而不是针对用户赋权。首先设置“教师组”对“教务处”文件夹有访问权限(一般把对资源的权限赋予给本地域组)，这样 user1 就有了对资源的访问权限(本地域组的成员可以包括账户)；然后再把“艺术系组”设置属于“教师组”(本地域组的成员也可以包括域中的其他组)，这样“艺术系组”中的所有成员都可以对“教务处”文件夹进行访问。

1.4.4　用户的概念

在网络上控制不同用户访问权限的方法是为用户设置账户，同时提供用户名和密码。每个用户都必须有一个账户，才能利用该账户登录到某台计算机，访问该计算机内的资源，或者利用账户登录到域，访问网络上的资源。

Windows 2003 所支持的用户账户分为两种类型：本地用户账户和域用户账户。本地用户账户前面已经介绍过了，这里不再重复。下面介绍域用户。

域用户账户建立在域控制器的 Active Directory 数据库内。用户可以利用域用户账户来登录域，并访问网络上的资源。用户可以在加入域的任何计算机上登录域(如果是域控制器，情况比较特殊，需要该域用户属于特权组)，系统会把用户提供的密码和 Active Directory 存储的该用户的密码进行比对，如果一致，便可以访问域中的资源。这样域中的所有计算机上都不必存储该用户的账户。这是一种集中化的管理方式，适用于用户、计算机比较多的情况。

例如，在一个 A. com 域中有 20 台计算机，新来的员工小张需要访问这 20 台计算机中的各种资源。如果采用本地账户类型，那小张不得不在 20 台计算机中建立 20 次“小张”这个账号，而且每次密码最好相同，如果不同，“小张”记忆起来比较困难。即使在 20 台计算机上建立了账号和统一的密码，如果某一天小张需要更改自己的密码，就不得不再跑到这 20 台计算机前，进行密码更改工作。显然，对于 20 台计算机的环境，这种本地账户类型已经暴露出明显的弊端，如果企业计算机是 100 台，那么采用本地账户类型简

直是场无法部署的工作。

针对规模比较大的环境，一般采用域的模式，那么账户就是域用户账户。还举上面的例子，小张只需要在域控制器(DC)上建立自己的域用户账号，就可以去访问这20台计算机的资源，而不用到20台计算机上分别设置账号，减轻了工作负担，提高了效率。即使以后小张为了安全，想更改自己的密码，也只需要更改域控制器中存储的密码即可。

1.5 活动目录的安装与卸载

1.5.1 活动目录的安装

通过1.4节的学习，对活动目录有了一个大致的了解，现在可以进行活动目录的安装与配置了。活动目录的安装配置过程并不是很复杂，因为系统提供了安装向导，只需按照提示一步步按系统要求设定即可。但安装前的准备工作比较复杂，只有充分理解了活动目录，才能正确地安装配置活动目录。

1. 活动目录安装前的准备

活动目录是Windows 2003系统中的一个关键服务，它不是孤立的，它与许多协议和服务有着非常紧密的关系，还涉及整个系统的系统结构和安全。安装活动目录不像安装一般的Windows组件那么简单，在安装前要进行一系列的策划和准备。

(1) 在安装活动目录之前，必须保证已经有一台计算机安装了Windows Server 2003，且至少有一个NTFS分区，而且已经为TCP/IP配置了DNS协议，并且DNS服务支持动态更新协议。

(2) 是要规划好整个系统的域结构。活动目录可包含一个或多个域，如果整个系统的目录结构规划得不好，层次不清就不能很好地发挥活动目录的优越性。

(3) 要进行域和账户命名策划。因为使用活动目录的意义之一就在于使内、外部网络使用统一的目录服务，采用统一的命名方案，以方便网络管理和商务往来。活动目录命名策略是企业规划网络系统的第一个步骤，命名策略直接影响到网络的基本结构，甚至影响网络的性能和可扩展性。活动目录为现代企业提供了很好的参考模型，既考虑到了企业的多层次结构，也考虑到了企业的分布式特性，甚至为直接接入Internet提供完全一致的命名模型。

(4) 要设置规划好域间的信任关系。在域树中创建域时，相邻域(父域和子域)之间自动建立信任关系。在域林中创建域时，在域林根域和添加到域林的每个域树的根域之间自动建立信任关系。如果这些信任关系是可传递的，则可以在域树或域林中的任何域之间进行用户和计算机的身份验证。

2. 安装活动目录

下面介绍建立整个网络的第一个域，即根域的操作步骤。

(1) 选择“开始”→“运行”命令，如图1-40所示。

(2) 在“运行”对话框的“打开”文本框中输入dcpromo命令，如图1-41所示。

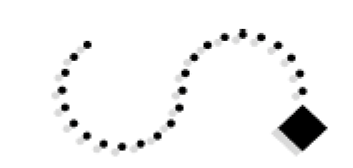




图 1-40　“运行”命令



图 1-41　输入 dcpromo

（3）在弹出的“Active Directory 安装向导”欢迎界面中，如图 1-42 所示，单击“下一步”按钮。

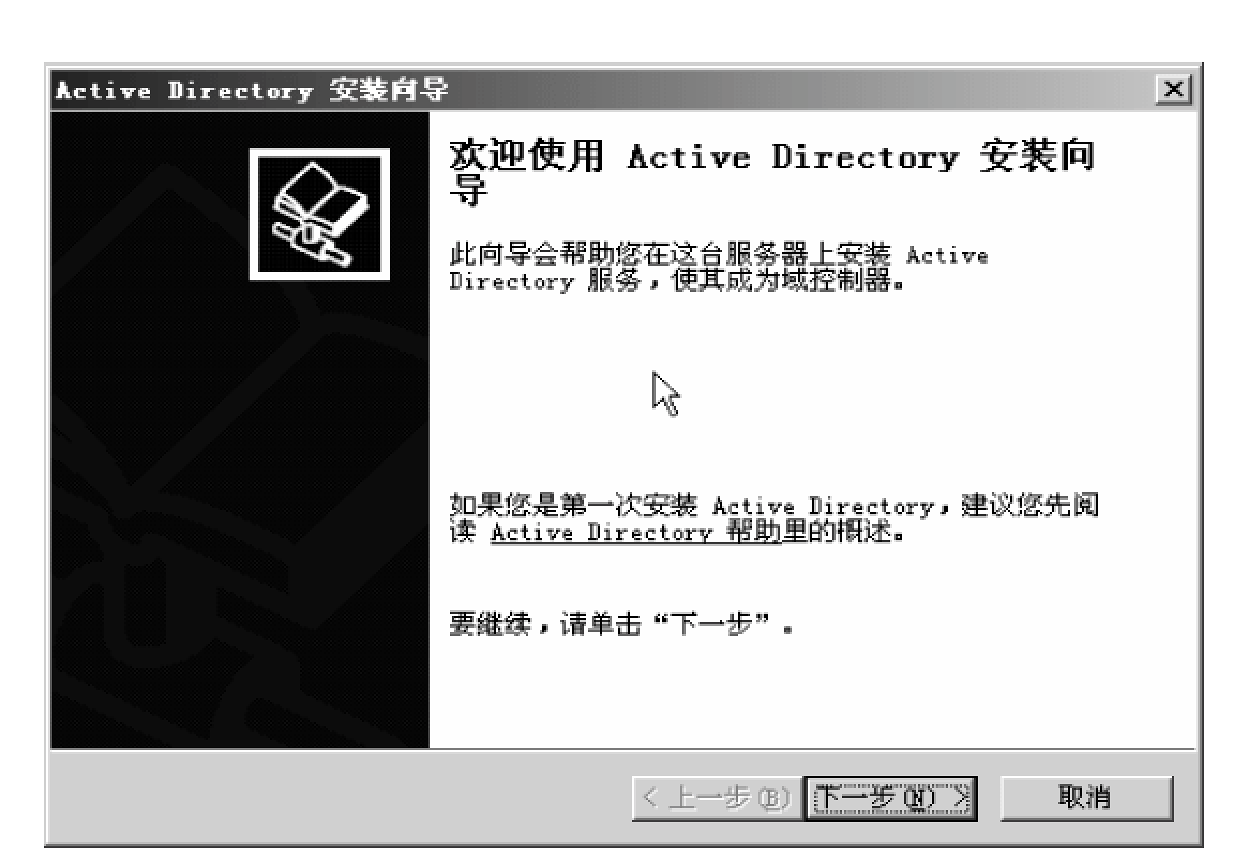


图 1-42　“Active Directory 安装向导”欢迎界面

（4）设置域控制器类型。选择“新域的域控制器”单选按钮，如图 1-43 所示，单击“下一步”按钮。

（5）选择“在新林中的域”单选按钮，如图 1-44 所示，单击“下一步”按钮。

（6）为新域指定域名。如果注册了域名，就输入注册域名全名，如 hqdx.com，如果还没有注册域名，输入 local.host 以示区别，如图 1-45 所示，单击“下一步”按钮。

（7）为新域指定 NetBIOS 域名。默认值是 DNS 名最左边的字符串，通常选择默认值，如图 1-46 所示，单击“下一步”按钮。

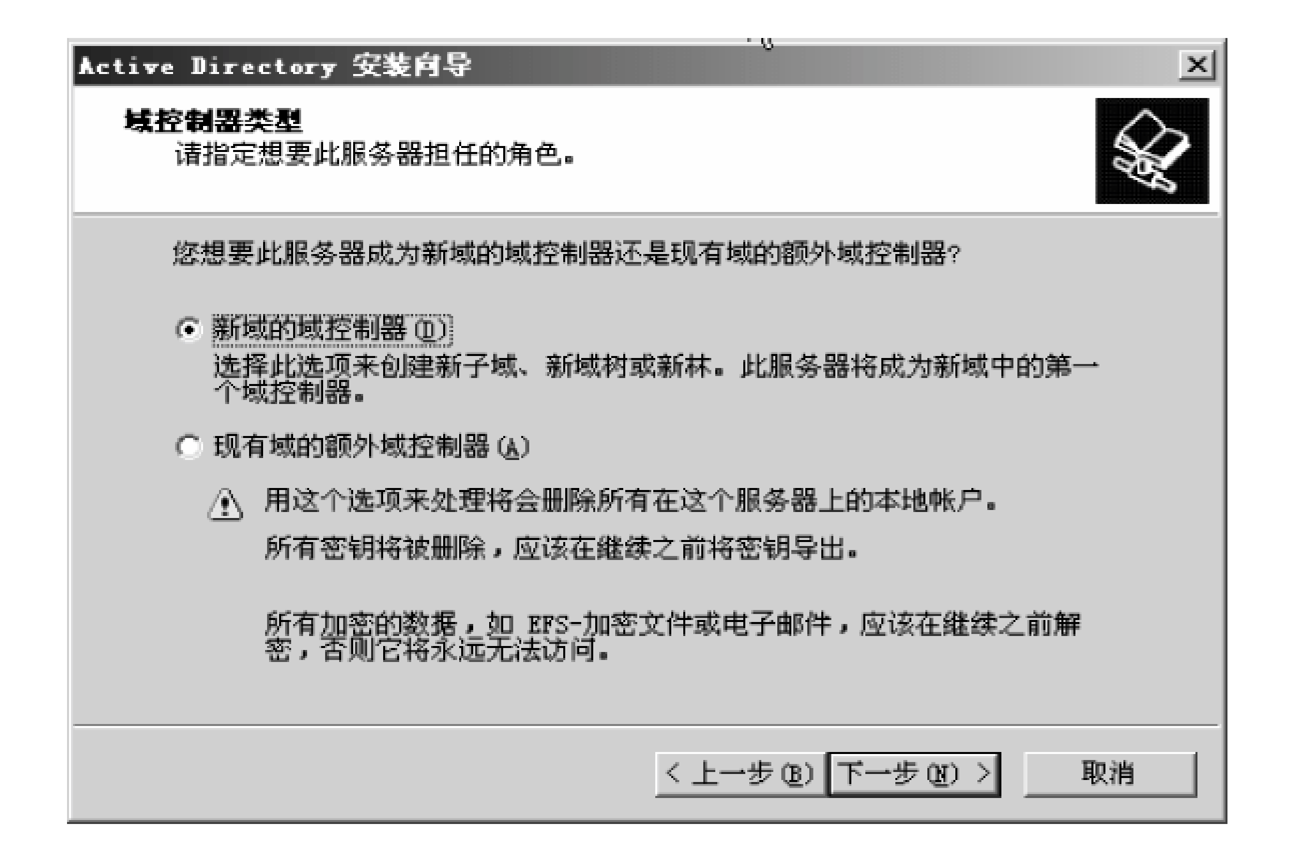


图 1-43　设置域控制器类型

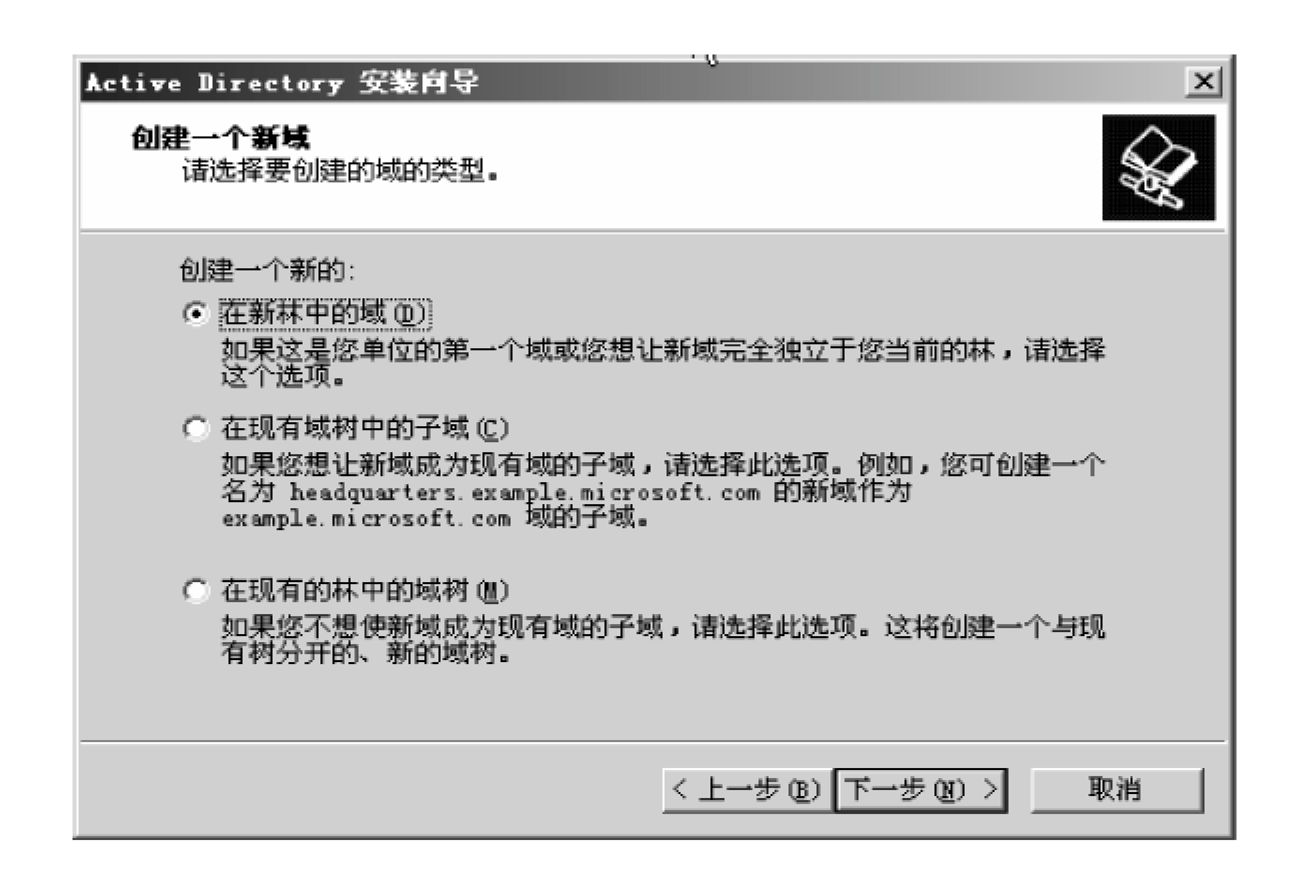
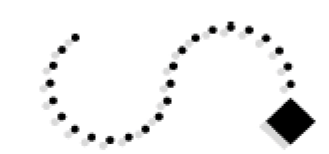


图 1-44　创建新域



图 1-45　输入域名



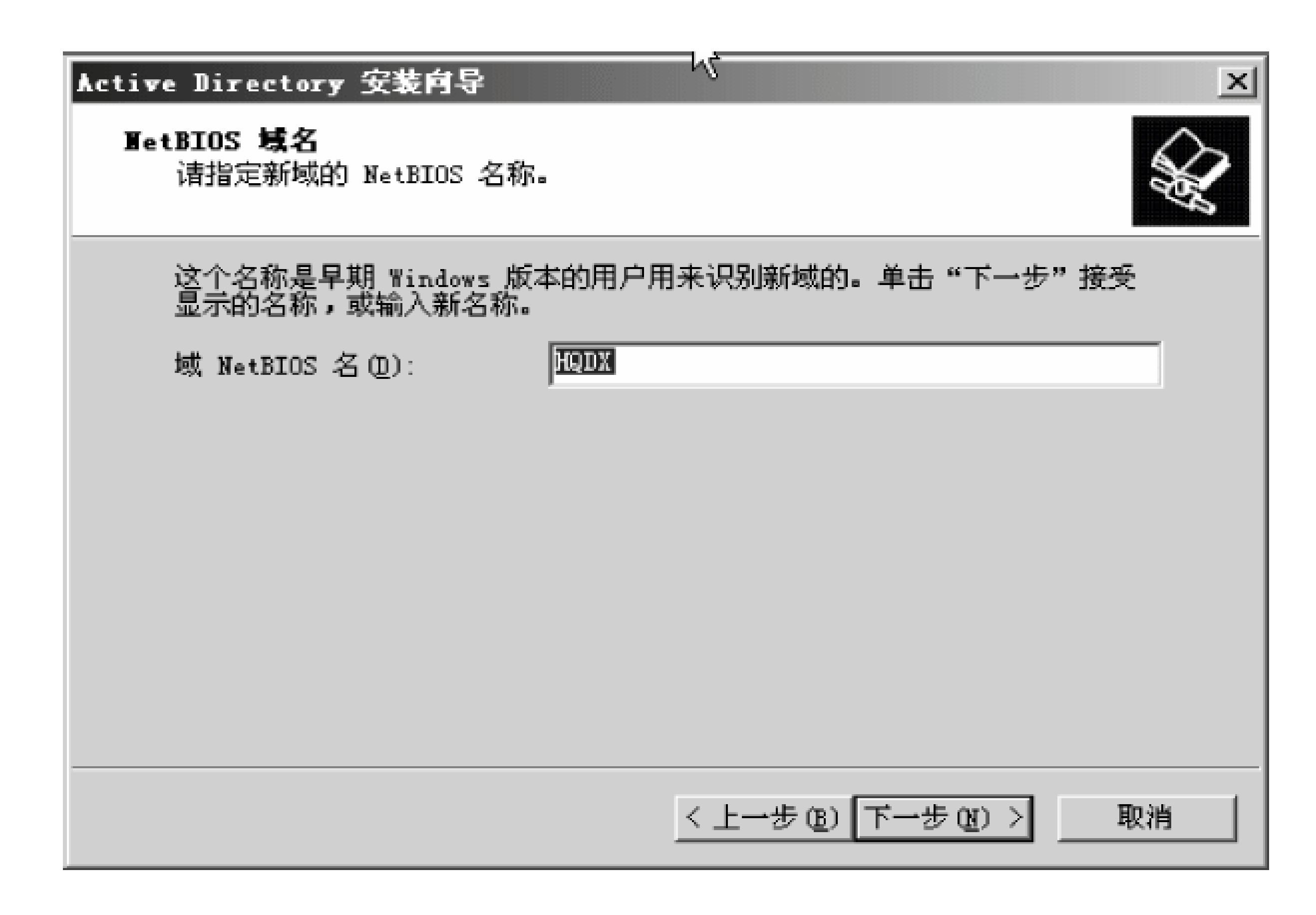


图 1-46　为新域指定 NetBIOS 域名

(8) 指定活动目录(AD)数据库和日志的存放位置。AD 数据库和 AD 日志最好分别存放在不同的硬盘上,可获得更好的性能。为了简化,也可以选择系统给出的默认位置,如图 1-47 所示,然后单击“下一步”按钮。

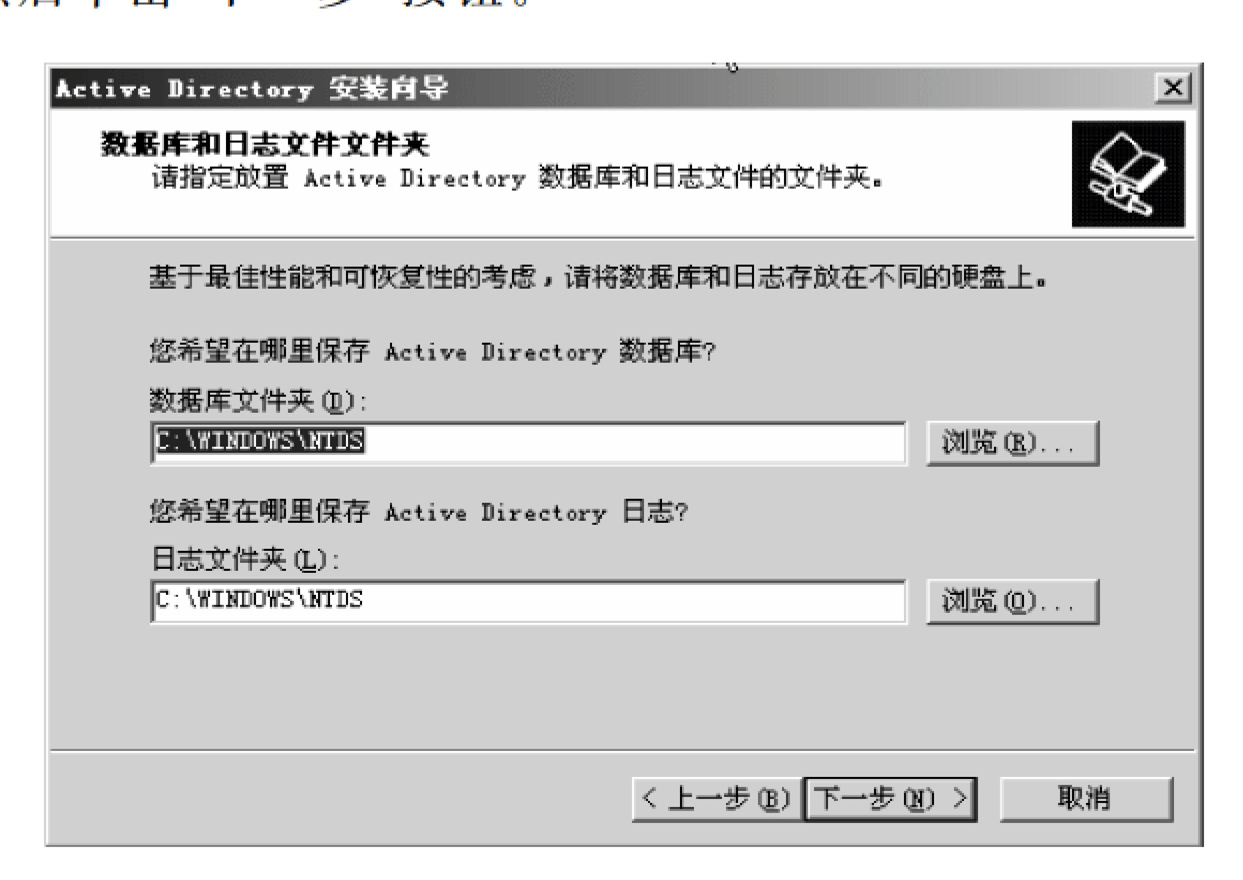


图 1-47　指定活动目录(AD)数据库和日志的默认的存放位置

如果想调整存放位置,可单击“浏览”按钮进行选择,如图 1-48 所示。

(9) 指定共享卷 SYSVOL 的存放位置,如图 1-49 所示。SYSVOL 文件夹存放域中公共文件的服务器副本。SYSVOL 中的内容将复制到域中所有的域控制器中。创建 SYSVOL 需要用 NTFS 格式化的卷,如果没有用 NTFS 格式化的卷,或者没有足够的磁盘空间,安装将不能顺利进行。然后单击“下一步”按钮。

(10) 配置 DNS 服务器。选择“在这台计算机上安装并配置 DNS 服务器,并将这台 DNS 服务器设为这台计算机的首选 DNS 服务器”单选按钮,如图 1-50 所示,单击“下一步”按钮。



图 1-48　指定活动目录(AD)数据库和日志的新的存放位置

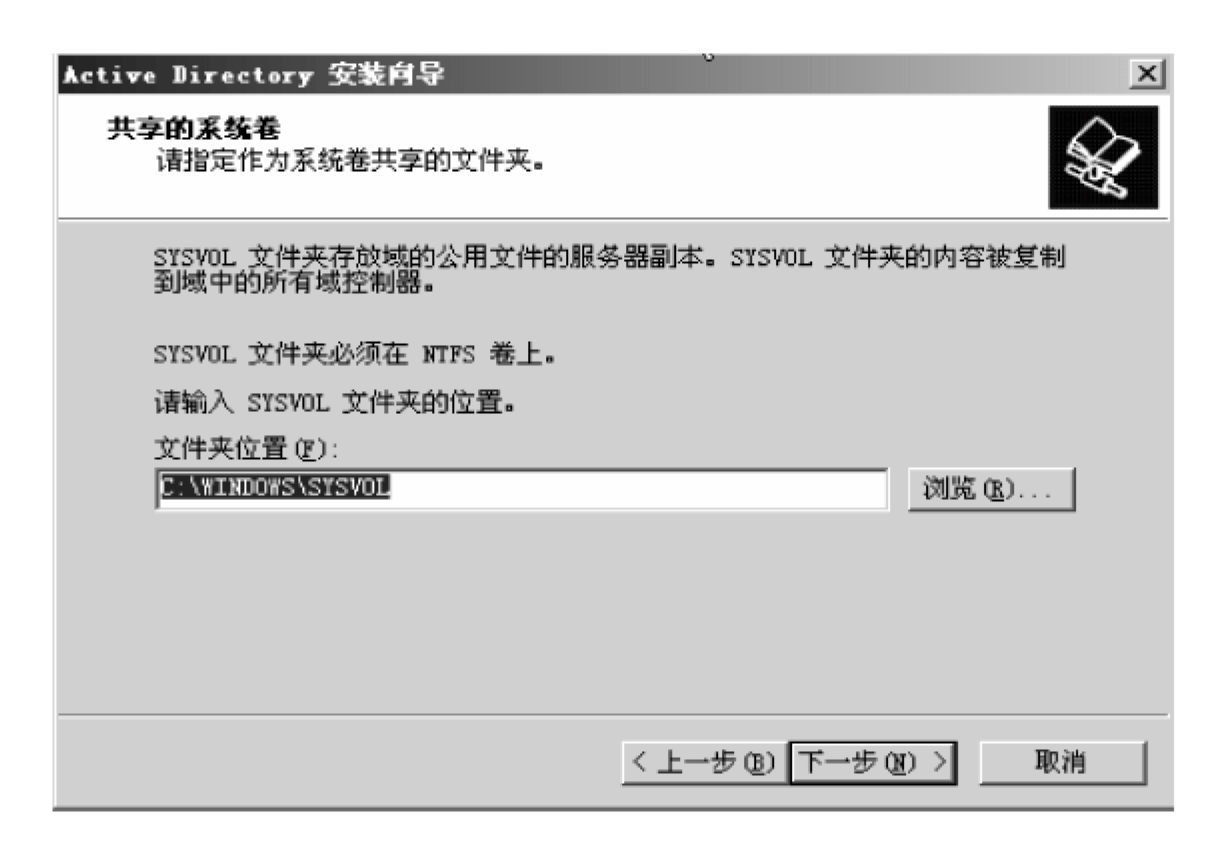


图 1-49　指定共享卷 SYSVOL 的存放位置

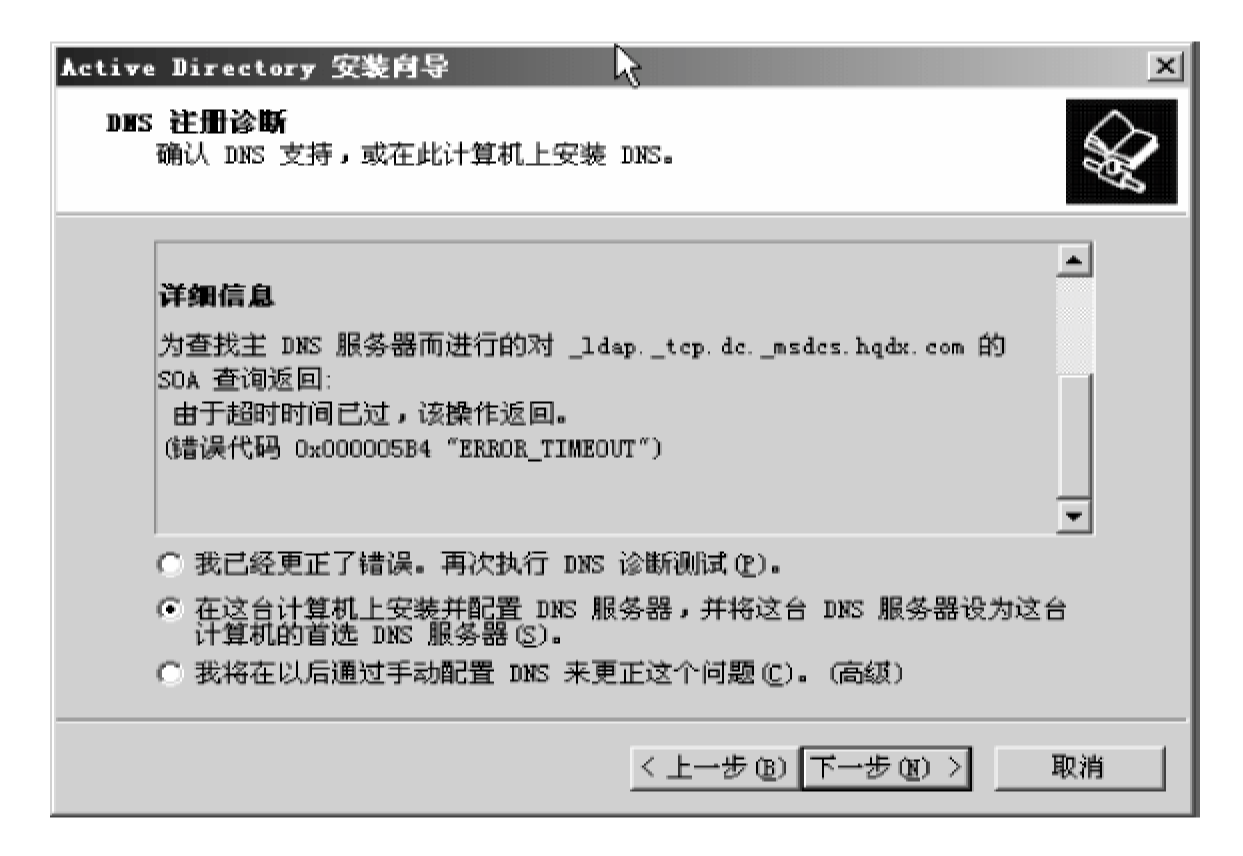
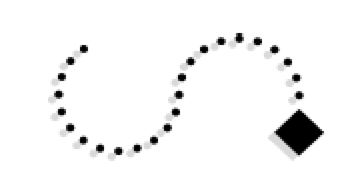


图 1-50　配置 DNS 服务器



注：此步骤是 Windows 2003 和 Windows 2000 的不同之处，在 Windows 2000 的 AD 安装过程中只是提示 DNS 不可用，让用户选择是在“本机安装”还是“事后安装”。

（11）选择用户和组对象的默认权限。建议选择“只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限”，如图 1-51 所示，单击“下一步”按钮。

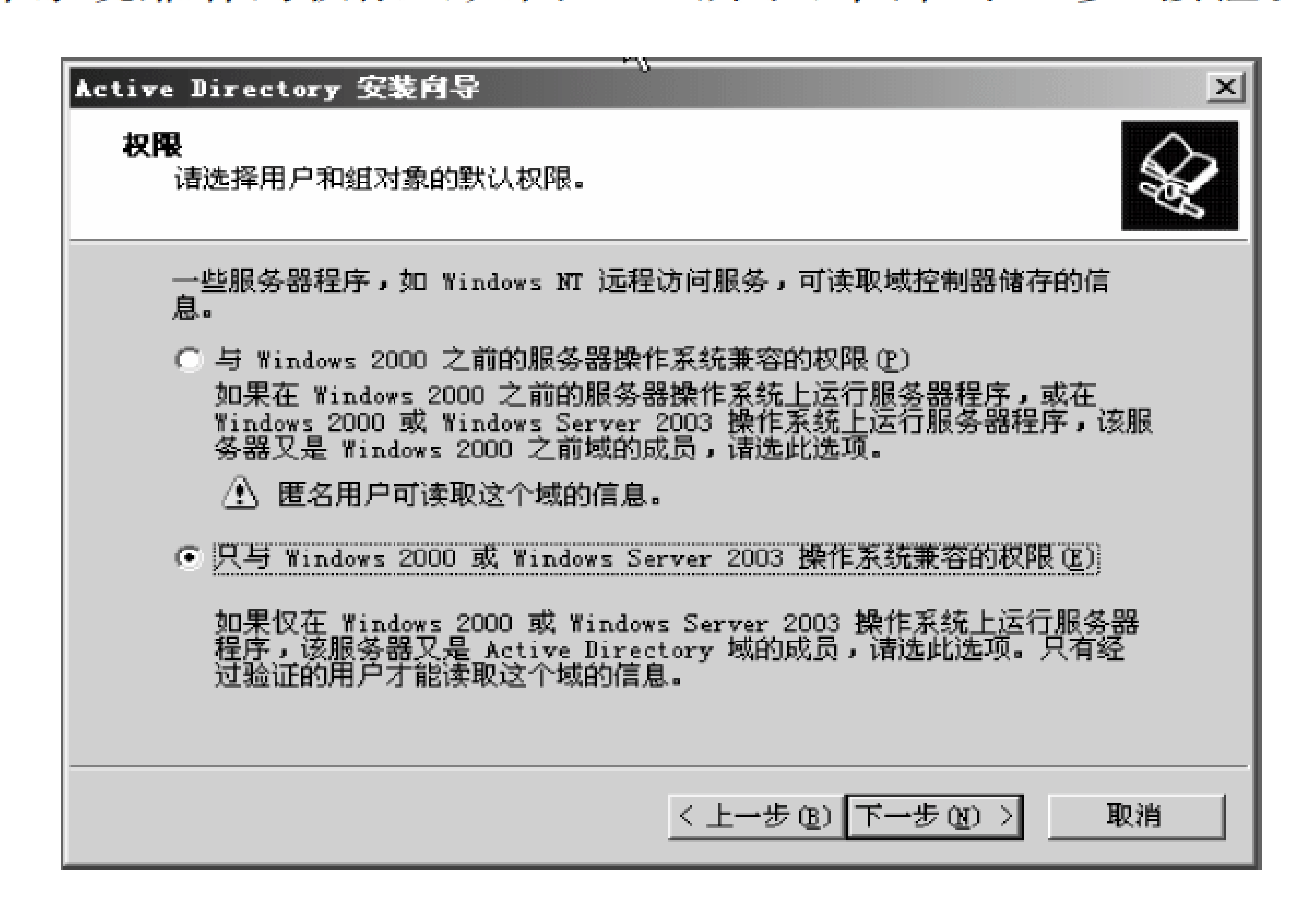


图 1-51　选择用户和组对象的默认权限

（12）设置目录服务还原模式的管理员密码。当活动目录数据被损坏时，可以在开机时按 F8 键，进入目录恢复模式，可重建 AD 数据库或者复制原来的 AD 数据。该密码是在进入目录恢复模式时所需的密码，如图 1-52 所示。单击“下一步”按钮。

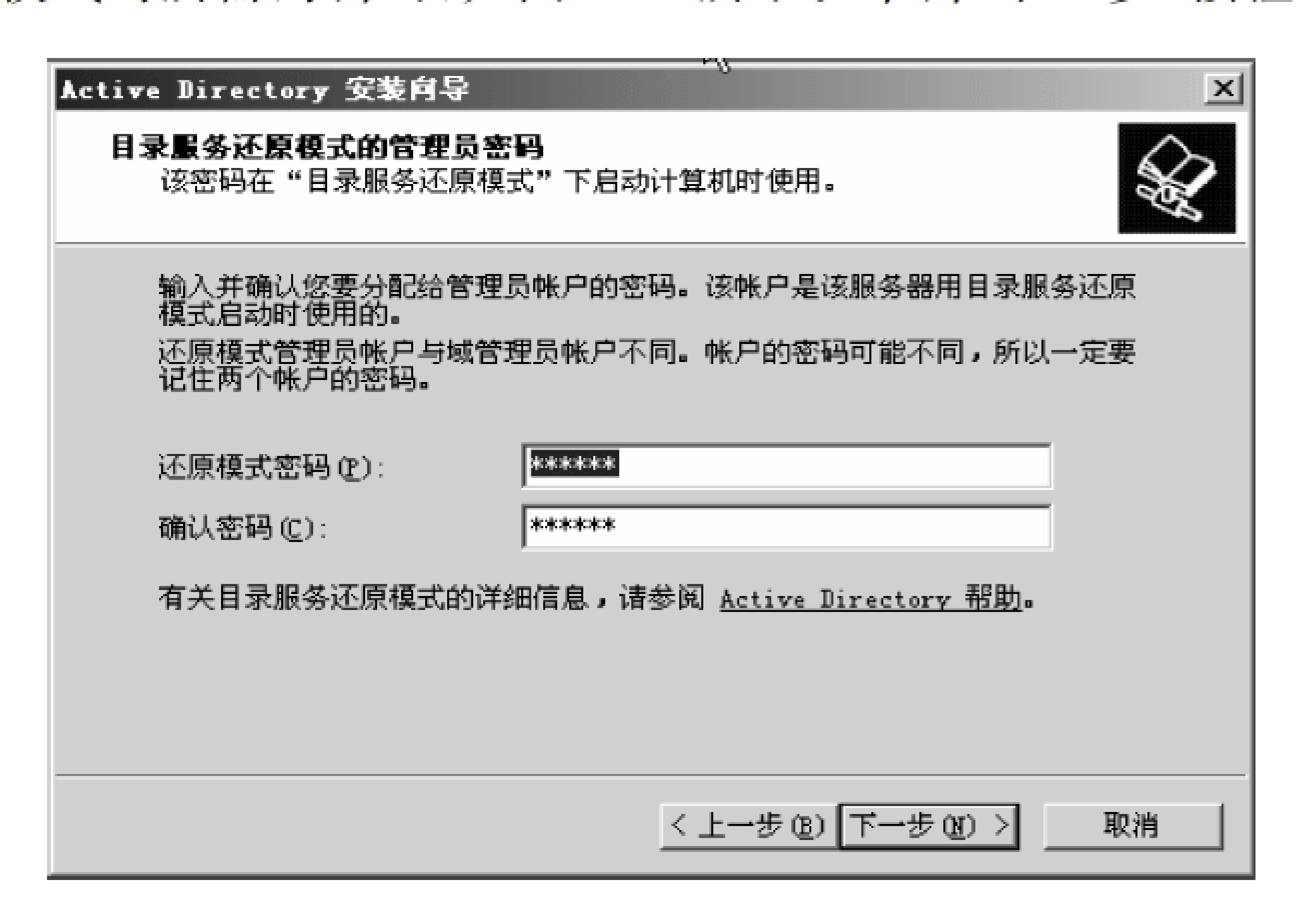


图 1-52　设置目录服务还原模式的管理员密码

（13）检查并确认选定的选项。对话框中显示前面所做的设置，如果没有改变，可单击“下一步”按钮，系统开始安装活动目录，如图 1-53 和图 1-54 所示。

（14）最后出现“完成安装”窗口，如图 1-55 所示，单击“完成”按钮完成活动目录的安装。

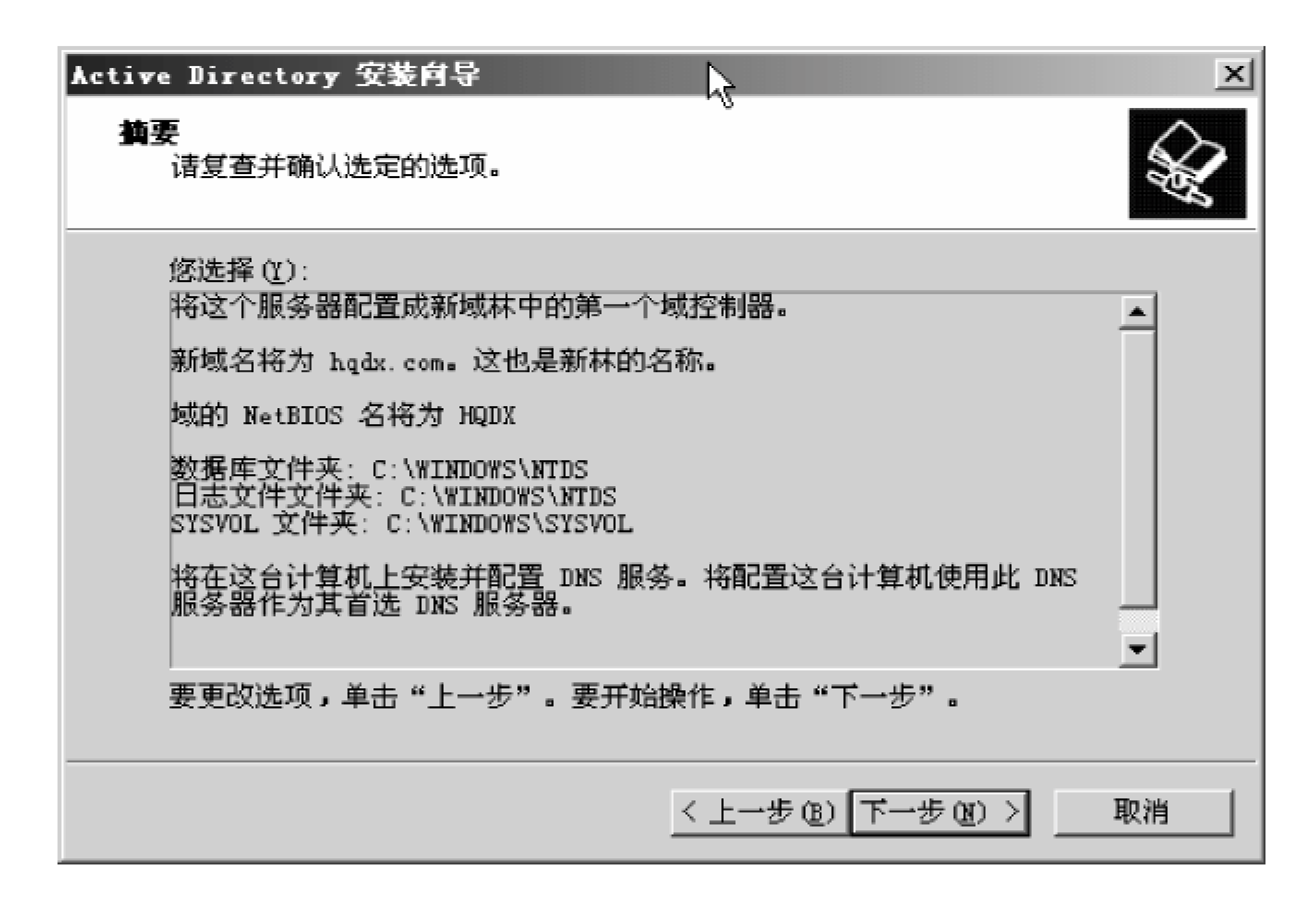


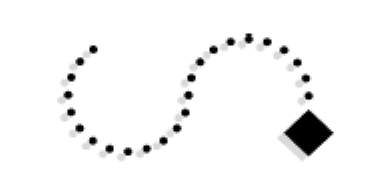
图 1-53　复查并确认选定的选项



图 1-54　向导开始安装 Active Directory



图 1-55　安装完成



（15）重新启动 Windows。单击“立即重新启动”按钮，如图 1-56 所示。只有重新启动，Active Directory 安装向导所做的设置才有效。



图 1-56　重新启动

（16）重新启动后，单击“开始”→“程序”→“管理工具”命令，可以看到“管理工具”菜单中增加“Active Directory 用户和计算机”、“Active Directory 域和信任关系”和“Active Directory 站点和服务”3 项，表示 AD 安装成功，如图 1-57 所示。



图 1-57　安装 AD 后，“管理工具”菜单中增加的项目

“Active Directory 用户和计算机”主要用于实施对域的管理；“Active Directory 域和信任关系”主要用于管理多域的关系；“Active Directory 站点和服务”一个是活动目录的域和域信任关系的管理，还有一个是活动目录的站点管理，可以把域控制器置于不同的站点。在一般局域网的范围内，为一个站点内的域控制器之间的复制是自动进行的；站点间的域控制器之间的复制需要管理员设定，以优化复制流量，提高可伸缩性。在活动目录管理界面中，还可以右击站点、域和组织单元，启动组策略(Group Policy)的管理界面，实施对对象的细致管理。

对于站点、域和组织单元，管理员还可以方便地进行管理授权。右击需要管理授权的站点、域和组织单元就可以启动管理授权向导，一步一步地设定哪些管理员对于哪些对象有什么样的管理权限。例如，企业内部技术支持中心的管理员，只有复位用户口令的权限，没有创建和删除用户账号的权限。这种更细致的管理方法称为“颗粒化”。

另外，活动目录还充分地考虑到了备份和恢复目录服务的需要，Windows 2003 备份工具中有专门备份活动目录的选项，在出现意外事故的时候，可以在计算机启动时按 F8 键进入安全恢复模式，保证减少灾难的恶性影响。

1.5.2　活动目录的卸载

（1）选择“开始”→“运行”命令，如图 1-58 所示。

（2）在“打开”文本框中输入 dcpromo，单击“确定”按钮，如图 1-59 所示。

（3）出现“Active Directory 安装向导”界面，单击“下一步”按钮，如图 1-60 所示。

（4）因为这台计算机是 hqdx.com 的域控制器，是一个全局目录服务器，所以出现一个提示对话框。单击“确定”按钮，如图 1-61 所示。



图 1-58 “运行”命令



图 1-59 输入 dcpromo

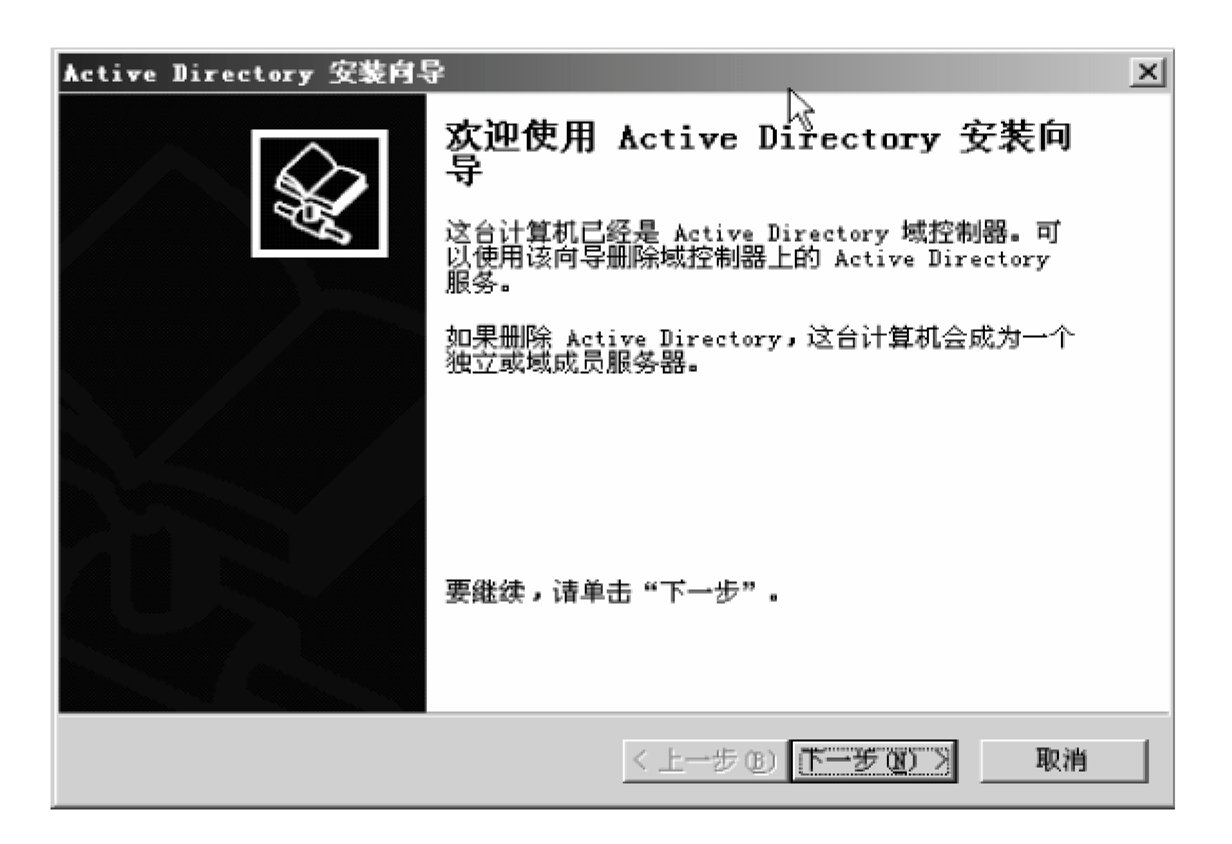
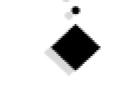


图 1-60 “Active Directory 安装向导”界面



图 1-61 提示此域控制器是全局目录服务器



(5) 指明这个域控制器是否是域中最后一个域控制器。如果这个域控制器是域中的最后一个域控制器,选择“这个服务器是域中最后一个域控制器”复选框,单击“下一步”按钮。如果这个域控制器不是域中最后一个域控制器,则直接单击“下一步”按钮,如图 1-62 所示。

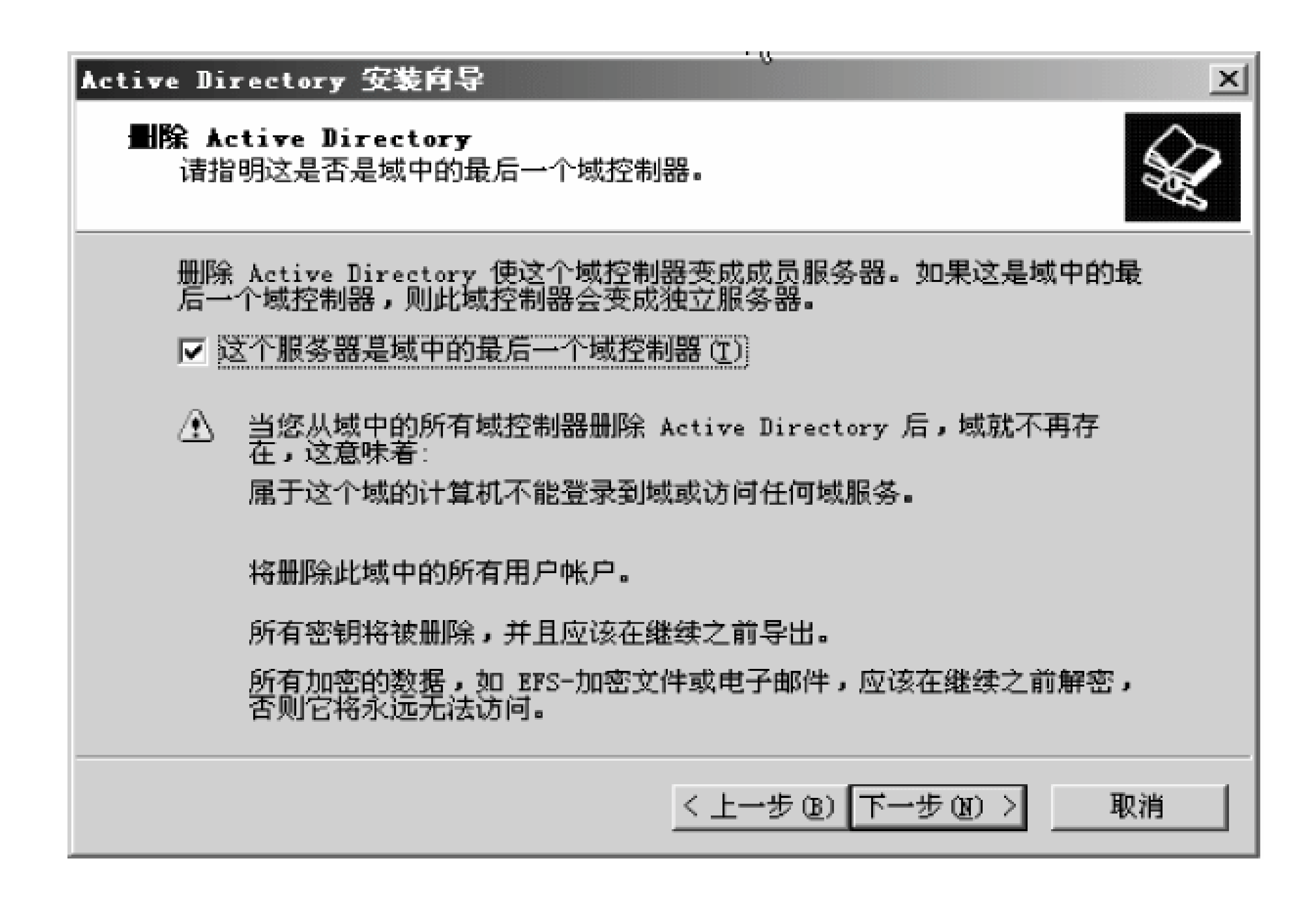


图 1-62　指明这是否是域中最后一个域控制器

(6) 出现“应用程序目录分区”窗口,这是由于一些应用程序在活动目录中创建了一些分区和存储了一些数据。单击“下一步”按钮,如图 1-63 所示。



图 1-63　应用程序目录分区

(7) 确认删除。选择“删除这个域控制器上的所有应用程序目录分区”复选框,单击“下一步”按钮,如图 1-64 所示。

(8) 出现“管理员密码”窗口,如图 1-65 所示。因为这台计算机是域控制器,只要有域用户的账号和密码,卸载活动目录后,域用户将消失,所以这里要求用户输入卸载域后

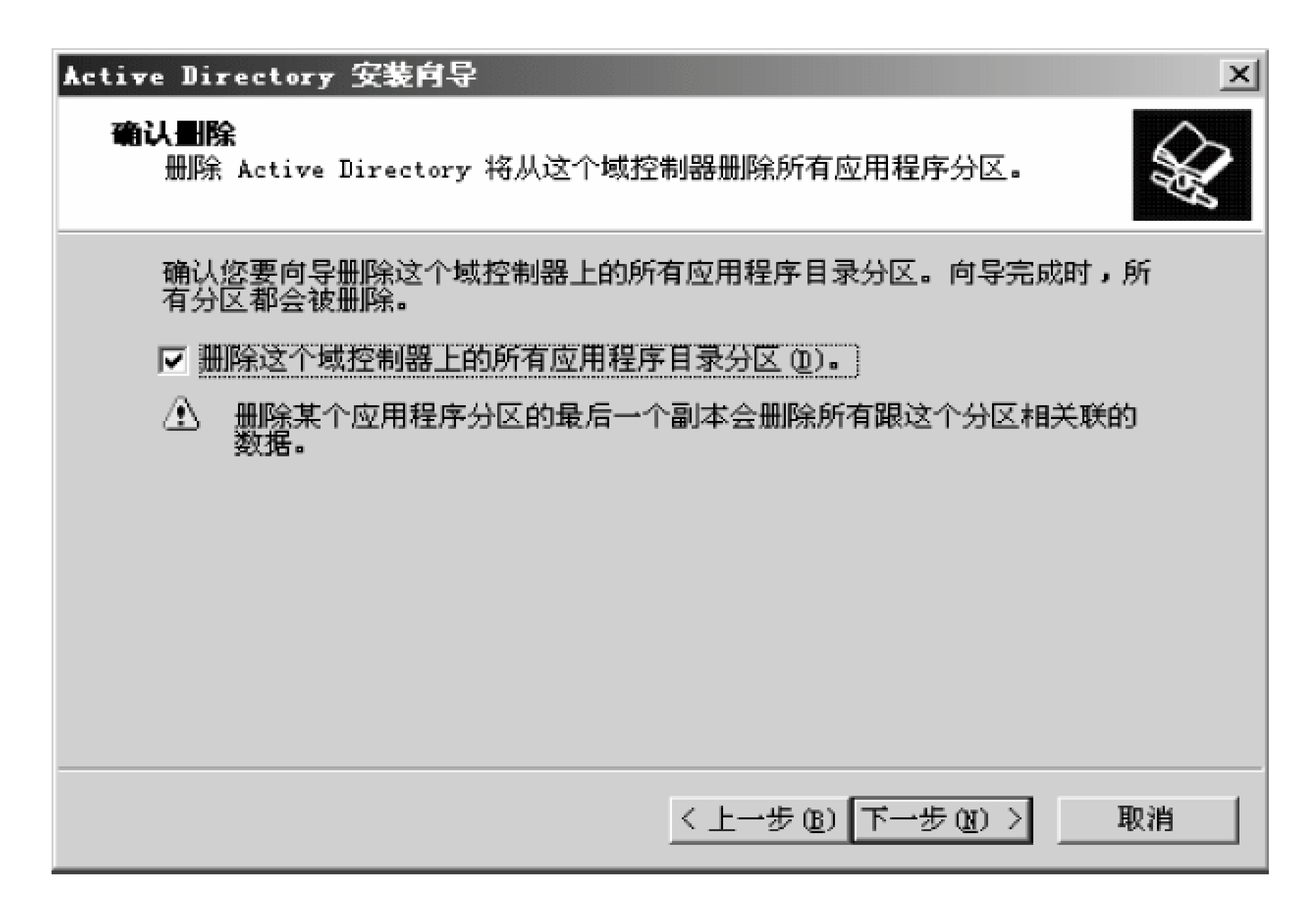


图 1-64　确认删除域控制器

图 1-65　输入卸载活动目录后计算机的管理员密码

的本机管理员的密码。密码要求由数字、字母和特殊符号组成，这样的密码比较安全。单击“下一步”按钮。

注：如果密码设置比较简单，则不能继续到下一个步骤。

(9) 复查并确认选定的选项。对话框中显示了用户选择的选项，如果不需要更改选项，可单击“下一步”按钮，系统开始卸载活动目录，如图 1-66 所示。

(10) Active Directory 的卸载过程根据计算机的配置不同，一般要持续一定时间，如图 1-67 所示。

(11) 最后出现完成 Active Directory 安装向导窗口，单击“完成”按钮，如图 1-68 所示。

(12) 单击“立即重新启动”按钮，如图 1-69 所示，完成活动目录的卸载。

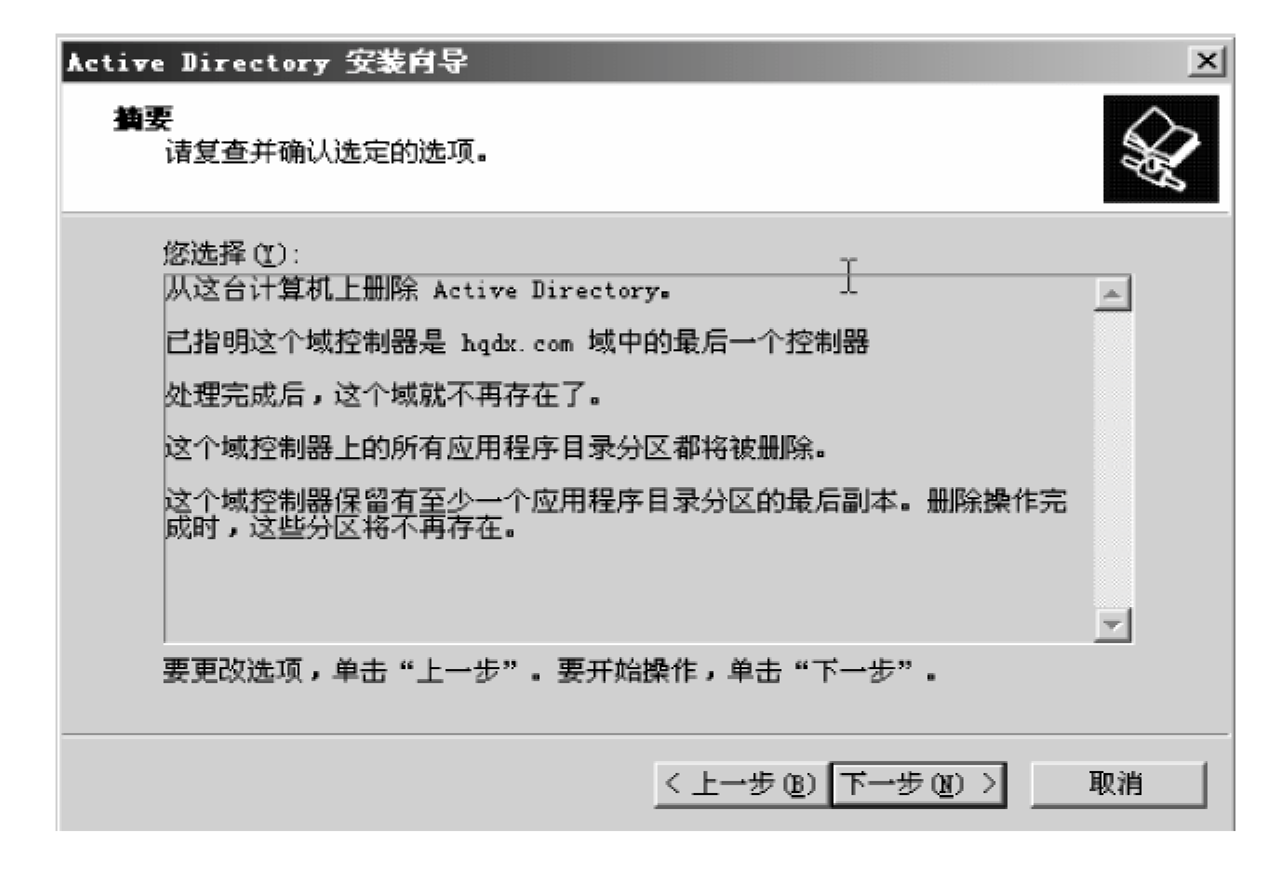


图 1-66　确认卸载



图 1-67　卸载过程



图 1-68　卸载完成



图 1-69　重新启动

1.6　本章小结

本章主要介绍了网络操作系统的概念，讲解了在操作系统的干预下各种网络的工作模式的特点及主要构成形式，同时介绍了如何用 Windows XP 进行对等网组网以及活动目录的安装与卸载。活动目录是进行域模式管理的基础，其中包含的概念希望读者理解与掌握。域模式将在第 2 章进行使用。

1.7　本章习题

1. 说明工作组模式管理和域模式管理各自的优缺点及适应场合。
2. 域在活动目录中起什么样的作用？
3. 比较组和组织单位在使用场合上的区别。
4. 在局域网的硬件环境已完成的情况下，用 Windows XP 组网。
5. 说明本地用户和域用户在局域网环境下的区别。

第 2 章

Windows Server 2003 域模式下管理

【本章内容】

本章主要介绍 Windows Server 2003 在单域模式下的管理方法与手段。通过使用活动目录提供的管理工具,运用域、用户、组、组织单位、组策略等概念完成对网络中的资源和用户的管理。希望读者体会这种先进的管理思想与技术,并能在实践中自觉使用。

【本章重点】

① 理解使用活动目录进行局域网管理的基本思想。

② 掌握用户、组、组织单位设置和管理方法。

③ 掌握组策略的概念。

④ 学会用组策略对用户和计算机进行管理。

⑤ 了解域、组织单位、组之间的区别。

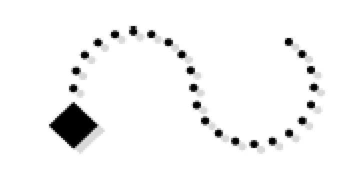
⑥ 通过实例的训练,掌握对局域网管理的实际操作方法。

第 1 章介绍了 Windows 2003 的工作模式,并在对等网模式下介绍了对局域网的管理。本章将详细介绍在单域模式下对局域网的管理。前提条件是已经在网络服务器上安装 Windows Server 2003 并配置了活动目录。对于多域等复杂情况,请读者参照有关资料进行学习。

2.1 设置和管理用户与组

第 1 章已经就 Windows Server 2003 不同的网络系统构架方式进行了详细的分析与系统的建立,并在建立的系统中完成了用户和组的设置与管理工作。本地机模式下的用户与组的管理,如图 2-1 所示。这时,每台计算机所构成的管理模式均是以当前计算机为主,所有对本计算机的访问和控制都要通过本地管理员账户完成,这个管理员账户就是系统提供的默认账户 administrator 和管理员组 administrators,网络中其他用户对当前计算机的访问设置也要在本地机中由管理员账户完成。

在一个小型网络中,计算机数量和用户数量有限,管理员还能够承担相应的工作,这



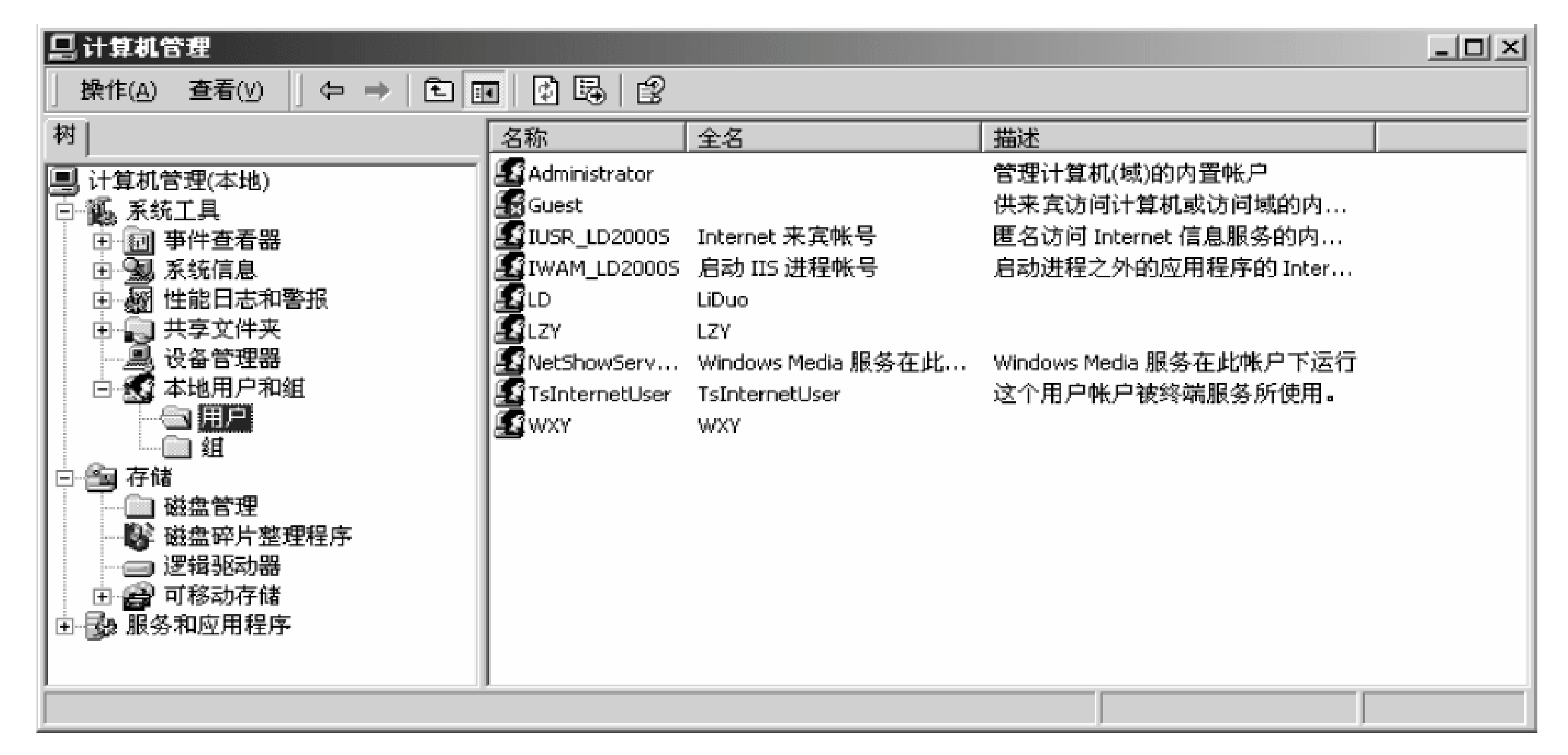


图 2-1 本地机模式下的用户与组的管理

时管理员要在服务器上为每一位访问该计算机的用户设置相关管理信息，这些管理信息包括对本地机的所有的安全方面的设置。随着用户对计算机使用需求的增加和改变，相关的管理工作会越来越复杂。

例如，现有一个安装了 Windows Server 2003 网络操作系统的网络环境，如图 2-2 所示。

在图 2-2 中，C 代表计算机，R 代表计算机用户。当每台计算机和每个用户构架出一个网络环境时，用户之间就要进行资源的共享和信息的传递。

当用户 R2、R3、R4 要使用计算机 C1 的资源时，必须由 C1 的管理员 R1 完成指定用户（R2、R3、R4 等）在本地计算机上的设置，如图 2-3 所示。

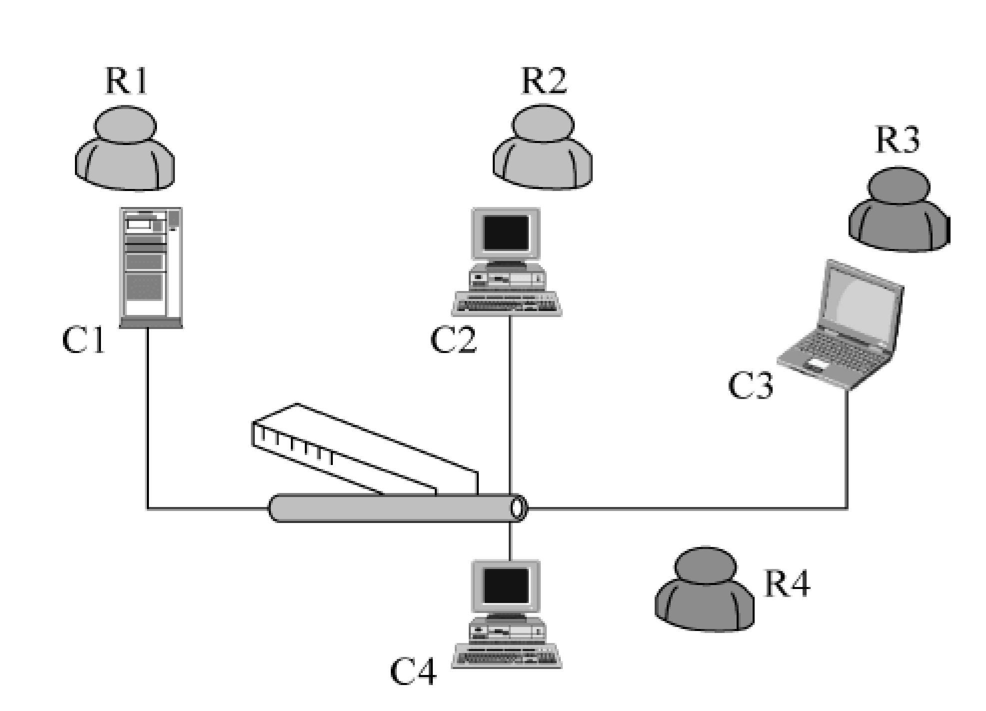


图 2-2 本地机模式下的用户对计算机的管理

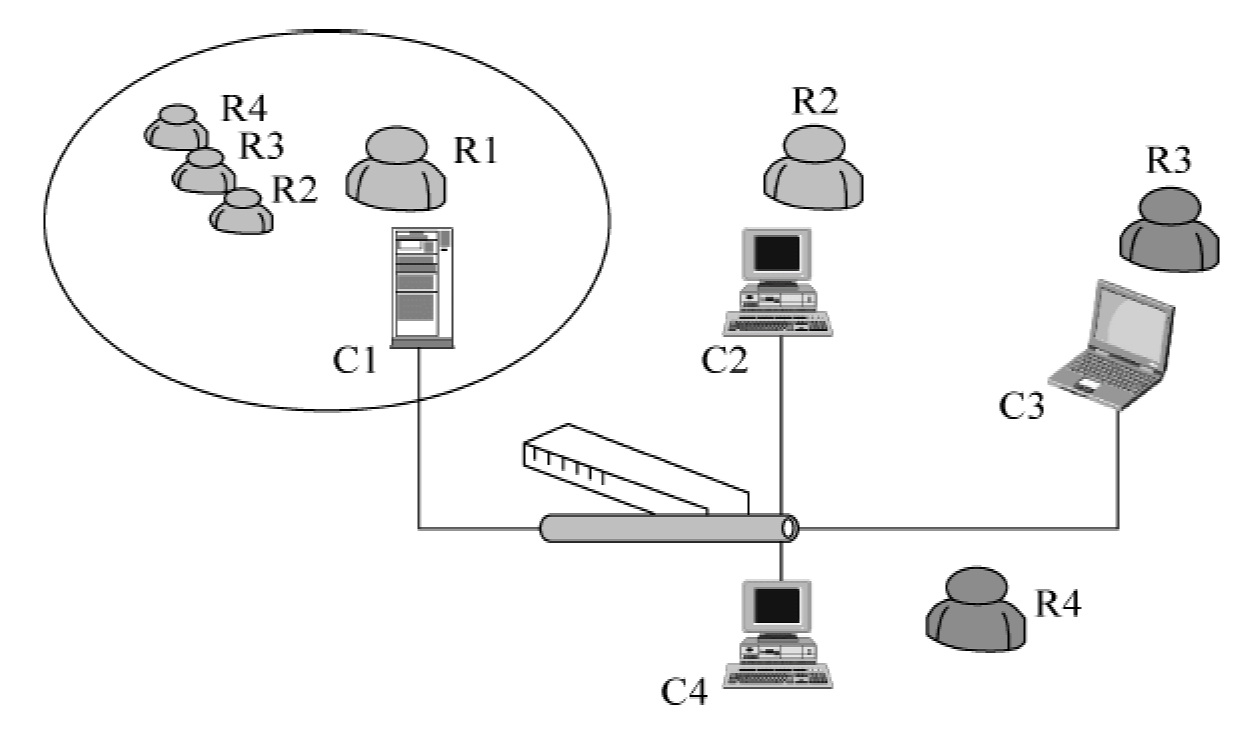
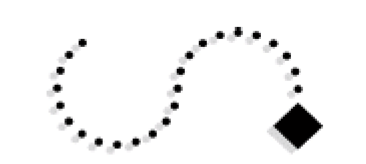


图 2-3 C1 计算机管理员 R1 对要访问该计算机的用户进行设置



当 R1 完成这些设置后，这些用户才能在计算机 C1 上使用权限所允许的功能。在这里，使用计算机 C1 的用户只是有限的几个用户，C1 的管理员可以完成相应的管理工作。如果每台计算机都有成百上千个用户，对每台计算机的管理员来说将是一场灾难，因为每个管理员要在自己的计算机上完成对要访问自己计算机的所有用户的管理设置，这个工作量将是繁杂重复的，如图 2-4 所示。

为此，引入域模式进行管理。

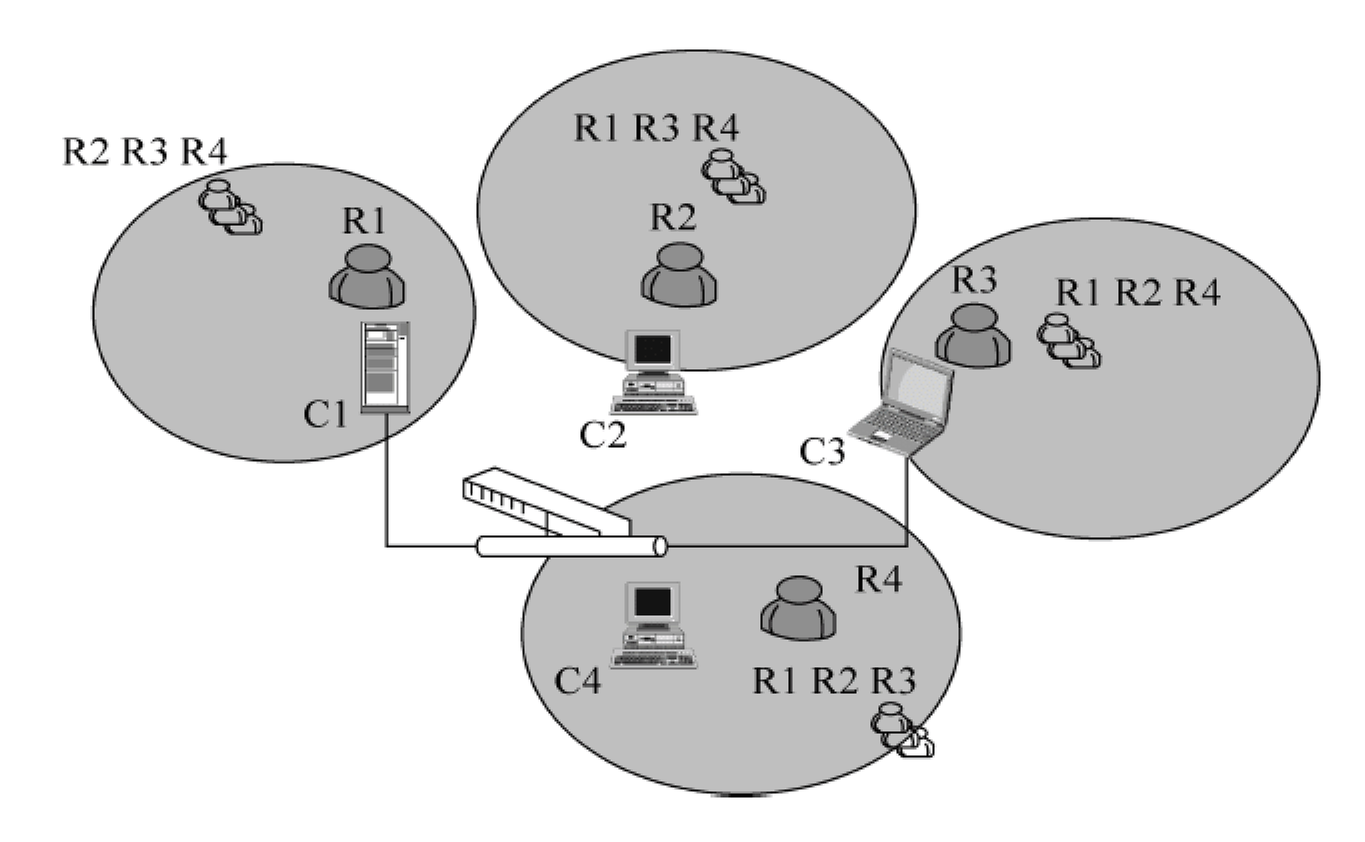


图 2-4　每台计算机管理员对所有要访问本地计算机的用户进行设置

2.1.1　域模式下用户的设置与管理

1. 域模式管理原理

微软公司在其网络操作系统中采用了域模式来改变原有的管理模式，提高管理效率。在第 1 章已经就域模式下的计算机管理系统做了详细的介绍，其核心就在于将计算机加入到一个指定的逻辑单元——域中，然后对加入其中的计算机实现统一、高效的管理，对整个网络系统中的计算机、用户、资源进行了重新的整合，使其在管理方式上发生了根本性的改变。

在域模式的管理体系下，整个网络管理经过以下 4 个过程实现对加入域的所有计算机和所有用户进行综合管理。

（1）建立一个域服务器，如图 2-5 所示。

（2）将被管理的计算机加入到域中，如图 2-6 所示。

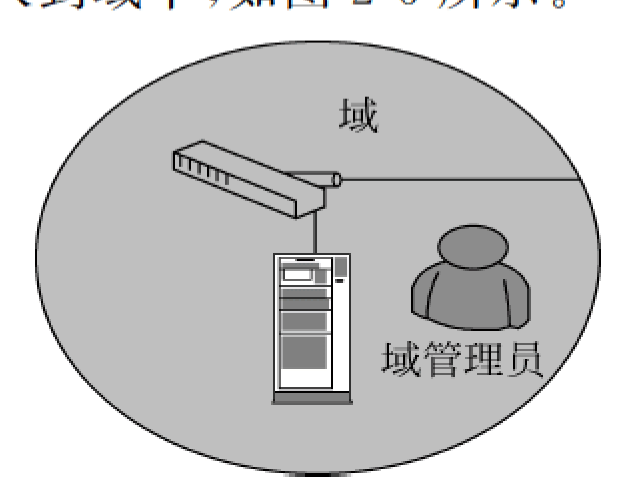


图 2-5　建立域和域管理员

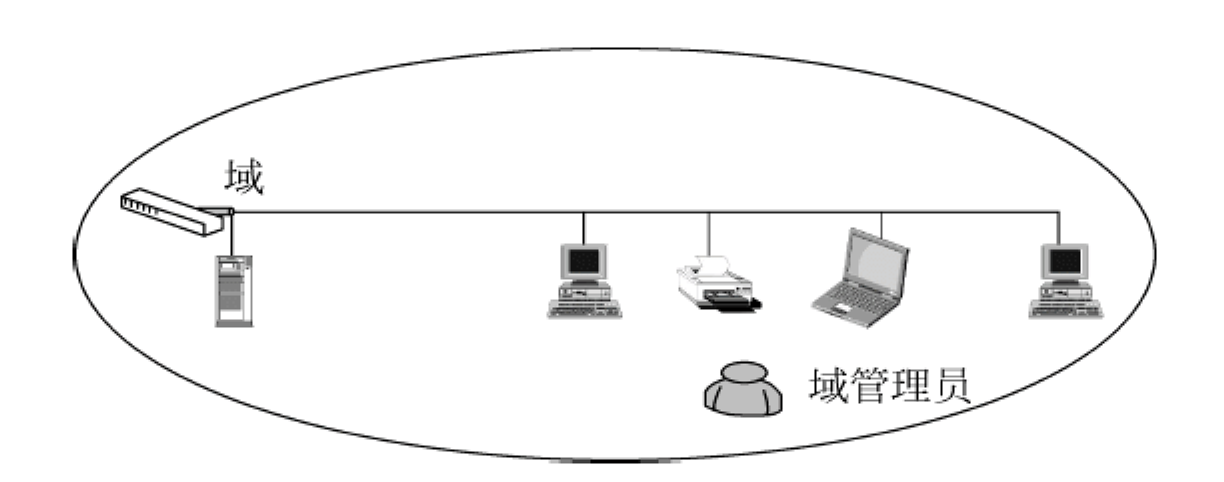


图 2-6　将计算机加入到指定的域中

（3）使用域下的管理员账户建立新的用户，如图 2-7 所示。

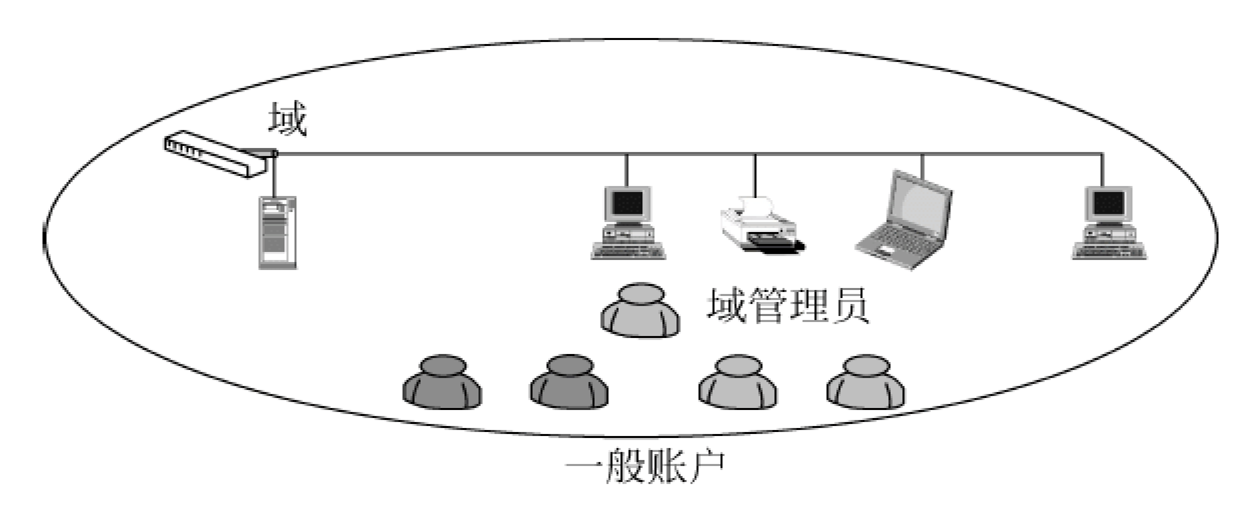


图 2-7　域管理员在域中任何计算机中创建账户

（4）在域中通过任何计算机对域中任何账户实现设置管理，如图 2-8 所示。

从以上步骤和图示中可以看出，当计算机加入到域成为域模式下的一台客户机时，针对该计算机的管理和针对用户的管理一下子就变得简单了，最终所有的用户都可以通过任意指定的计算机访问任意计算机上的文件夹，且可运行权限允许的可执行文件。

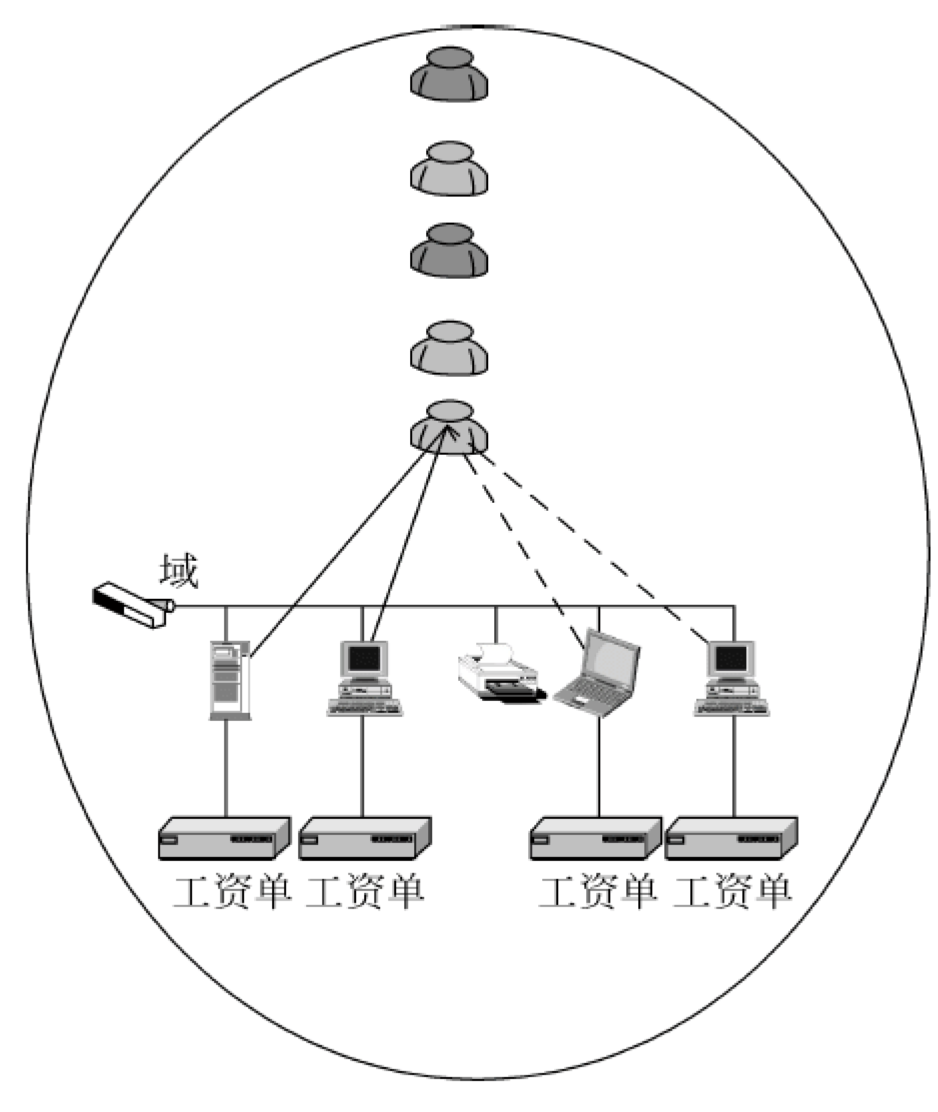


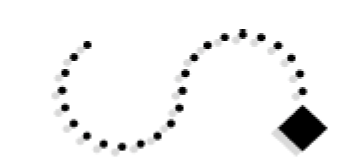
图 2-8　域中用户通过域中任何客户机访问权限允许的任何文件夹

2. 域模式下用户设置

当一台计算机成为域控制器时，或者当一台计算机加入的域成为域模式下的一台客户机时，每台计算机中的账户信息将发生改变。

（1）在域控制器中，原本地账户已经不能使用了。因为，原本地管理员的账户继续存在将有可能破坏域服务器，因此对域控制器的管理和控制交由域控制器管理员完成。进入域控制器管理界面的命令方法如图 2-9 所示。

当域管理员登录域控制器时，在域控制器中出现了新的账户管理界面。选择“开始”→“程序”→“管理工具”后出现了新的功能选项“Active Directory 用户和计算机”，如图 2-10 所示，选择该命令可进入域控制器账户的管理界面。



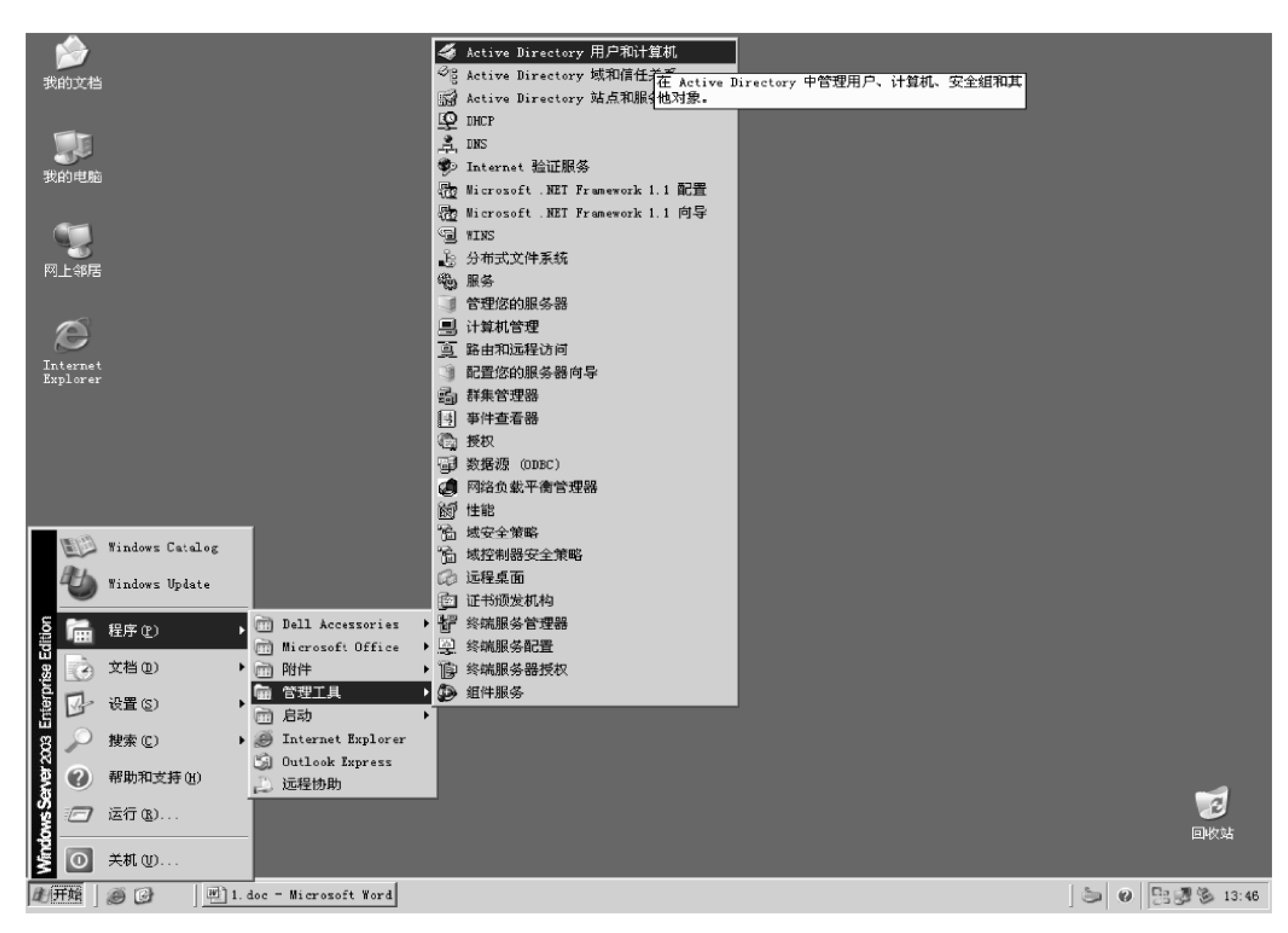


图 2-9 域控制器管理界面

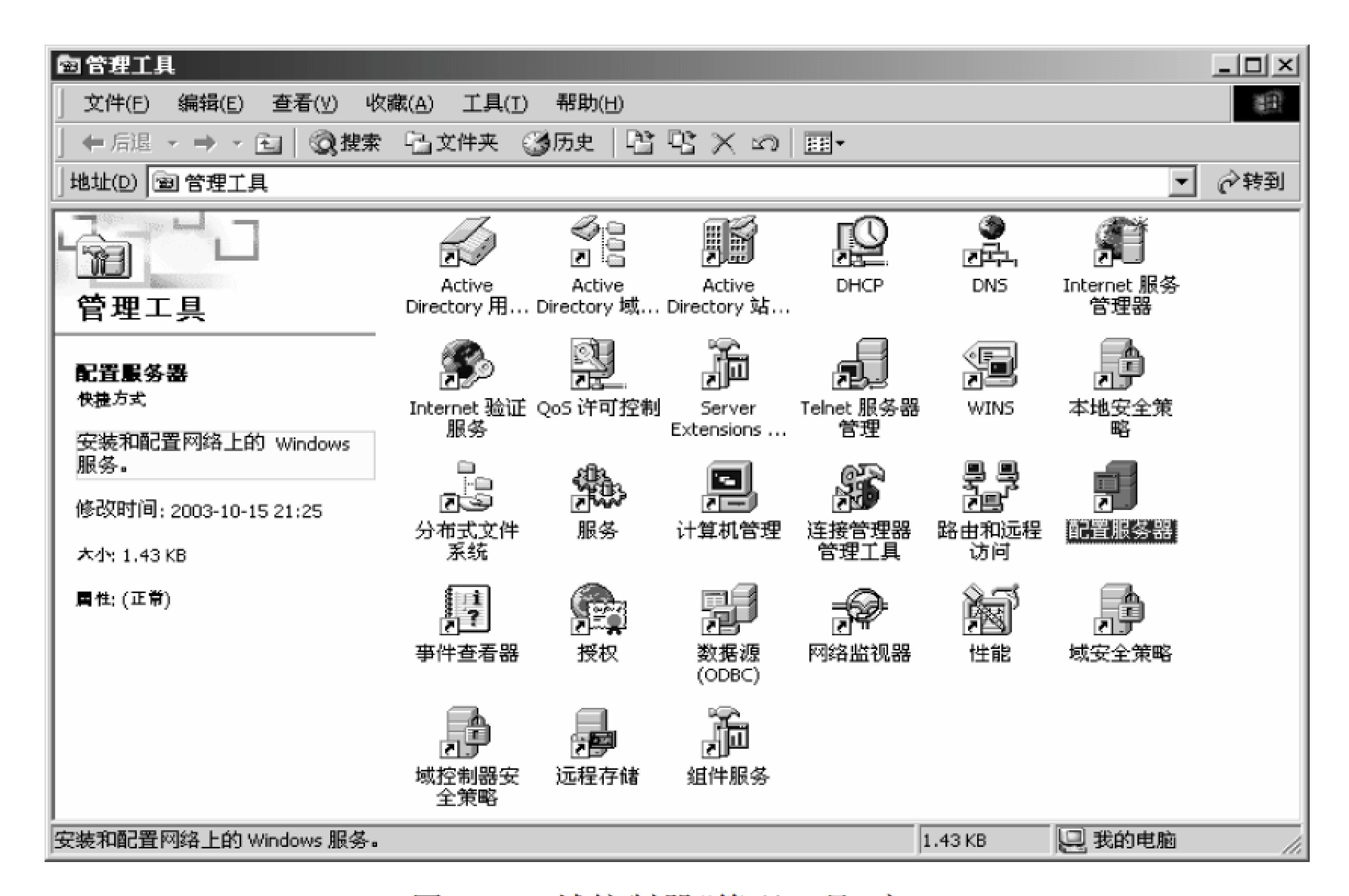


图 2-10 域控制器“管理工具”窗口

（2）通过客户机进入域控制器前，系统出现两个进入选项，一个是本地机进入选项，一个是域控制器选项，如图 2-11 所示。客户机如果不进入域则选择本地机选项，如果进入域则选择域选项。作为客户机的本地管理账户，仍然保留对本地计算机控制的权力。

（3）域模式下的默认账户。在域控制器中，与本地机情况相同，存在着系统创建的默认账户，这些账户有其特定的功能与权限，如图 2-12 所示。



图 2-11　客户机开机界面

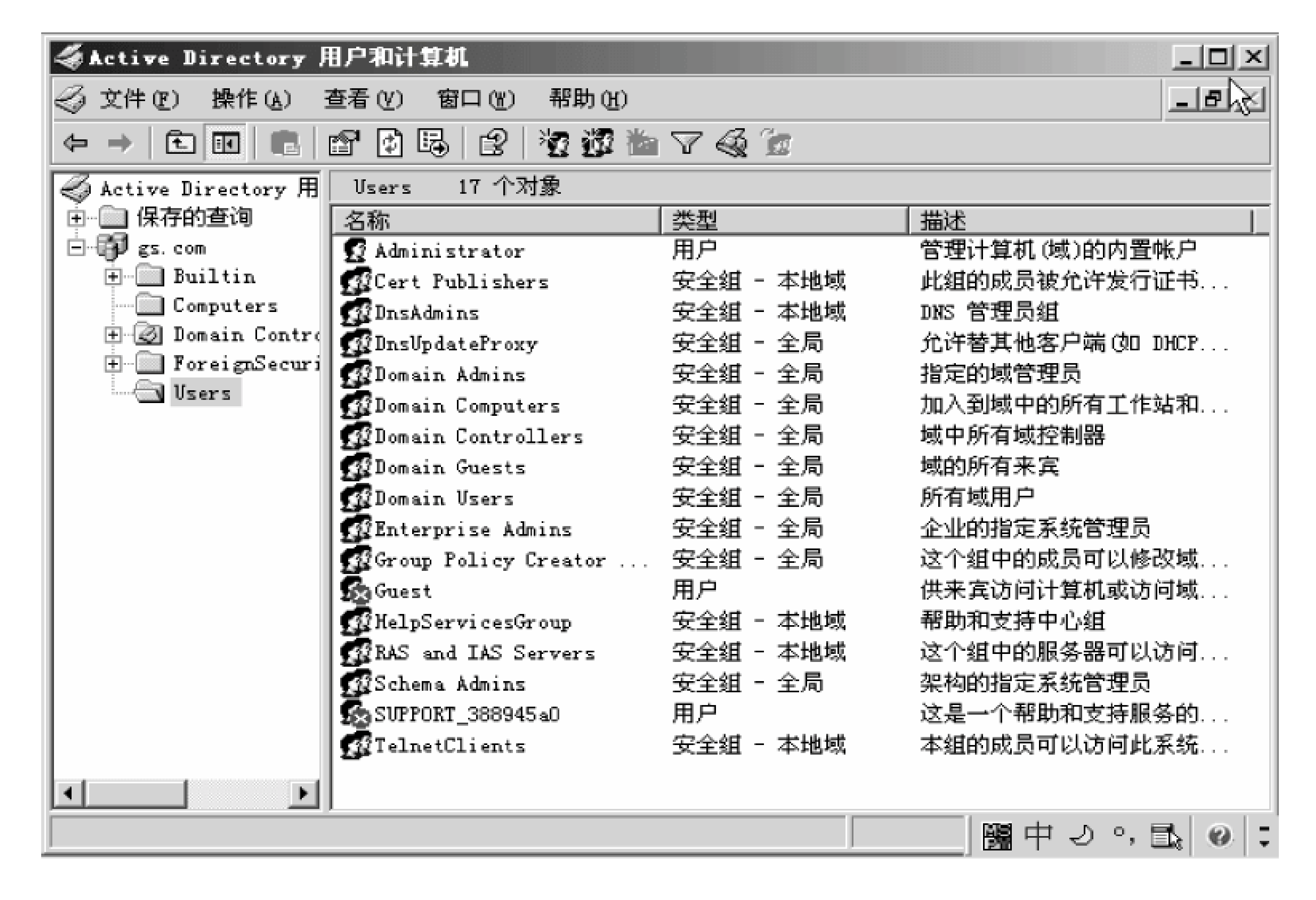


图 2-12　域控制器默认账户

对其中重要账户解释如下：

① Domain Admins（域管理员）用于域范围内的管理，拥有最高权限。

② Administrator（本地（域控制器）管理员）用于计算机（域）内置账户的管理。

（4）域模式下的账户建立，在已经安装完活动目录并且成为域控制器的服务器中，其用户是通过“Active Directory 用户和计算机”创建的。具体操作步骤如下：

① 打开“Active Directory 用户和计算机”窗口，在控制台下右击 User 容器，在弹出的快捷菜单中选择“新建”→“用户”命令，如图 2-13 所示。

② 在“新建对象—用户”对话框中输入用户的姓名及用户登录信息，如图 2-14 所示。

注意：在输入账户信息时，可以输入中文作为用户登录名。“用户登录名”文本框中输入的名字是该账户登录域时使用的名字，“姓”、“名”文本框中输入的内容只是作为账户登录信息，与登录域时输入的账号无关。

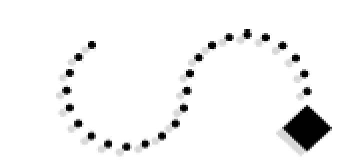




图 2-13 新账户创建

③ 单击“下一步”按钮为用户设置密码，其操作与第 1 章建立账户的操作相同，按照中文向导操作提示进行设置，如图 2-15 所示。



图 2-14 输入用户信息



图 2-15 输入账户信息

注意：建议密码不要设置成有规律的字母，因为这样的密码极易被网络攻击者猜中，降低了网络的安全防范能力。

在建立密码后对话框中有 4 个用来表示密码的设置方式的复选框。

- “用户下次登录时须更改密码”表示该账户第一次登录域中的计算机时，系统要求用户必须更改密码，这样保证用户自己掌握自身账户的密码。
- “用户不能更改密码”表示用户自己没有权利对自身账户密码进行修改，必须通过域控制器管理员来完成。

- “密码永不过期”表示账户设置的密码不会因系统默认的密码有效期到期而要求用户修改，密码始终有效。
- “账户已停用”表示当前账户如果不能在域中继续使用，可以使账户停用，而不是删除账户信息。

3. 域模式下的账户的管理

在基于域模式下的 Windows Server 2003 的账户信息变得异常丰富，域管理员被赋予了极大的权力，对于所有加入到域中用户的账户信息都要进行管理和维护，而账户信息将被域中所有有权需要账户信息的各个部门所使用。从这点可以看出，对域模式下的账户管理涵盖了用户的诸多信息，如图 2-16 所示。

（1）设置账户属性

在第 1 章已经就针对账户的一般性维护做了介绍，下面介绍基于域模式下的账户属性中的特殊部分。在账户属性对话框中有 16 个选项卡，涵盖了账户的大部分信息，下面分别介绍。

① “常规”、“地址”、“电话”、“单位”选项卡中的信息是账户的个人信息，用于拥有权限的账户查询，如图 2-16 所示。

② “账户”选项卡的上半部分与原普通账户信息没有区别，但下半部分包括了众多的信息，如图 2-17 所示。在域控制器管理的网络系统中，所有的账户可以被限制在以 5 种方式进入系统和运用系统，这种限制归纳为 5 个指定，即：

- 指定的账户——用户进入计算机的凭证。
- 指定的计算机——用户从指定的计算机进入系统。
- 指定的时间——用户在规定的时间进入系统。
- 运行指定的程序——用户只能调用指定的应用软件。
- 访问指定资源——用户只能访问指定的文件夹和对文件夹进行指定的处理。

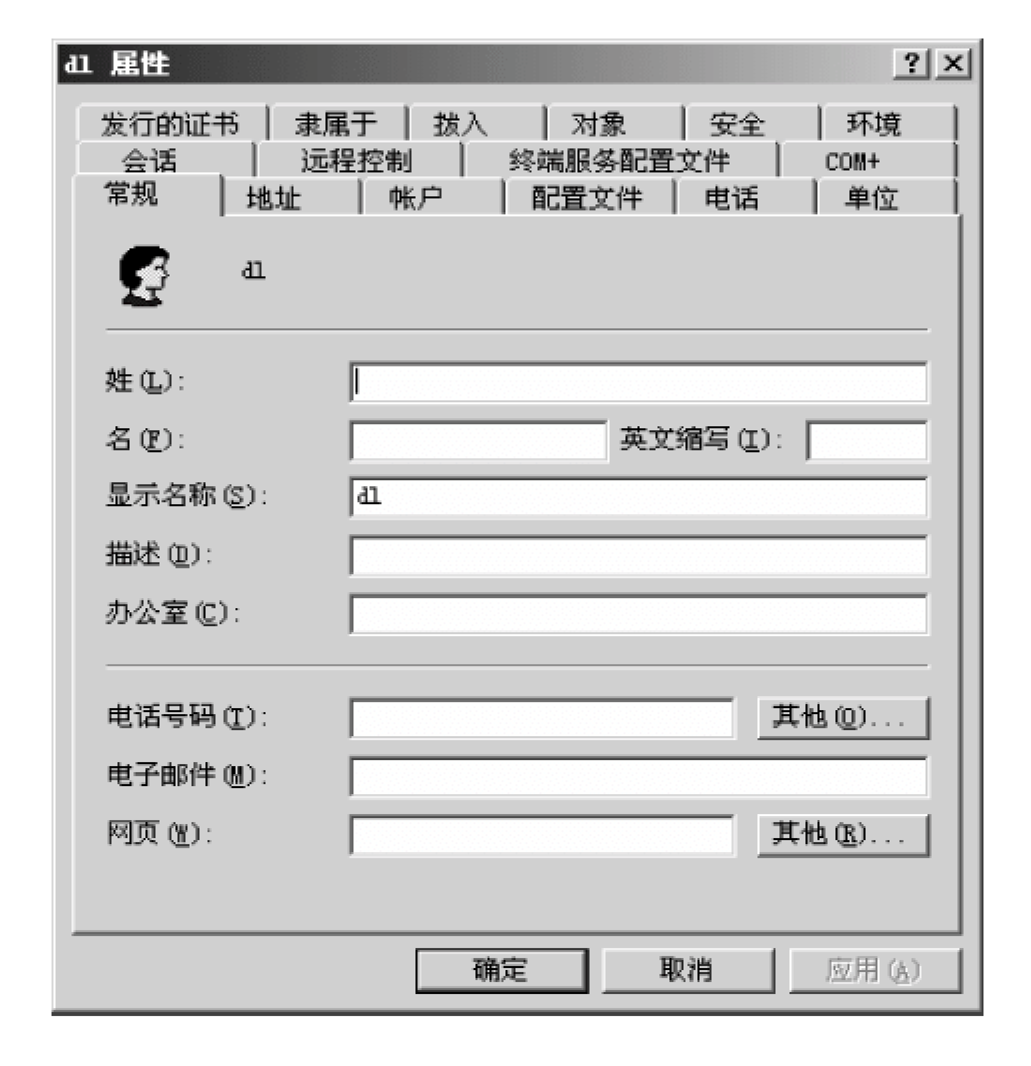
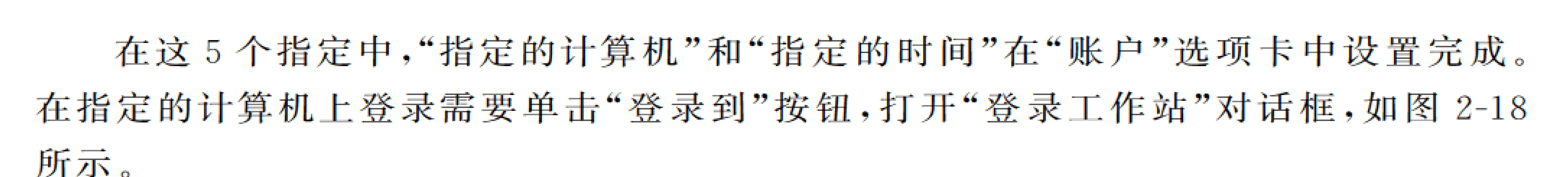


图 2-16　账户常规信息



图 2-17　账户信息



在这 5 个指定中,“指定的计算机”和“指定的时间”在“账户”选项卡中设置完成。在指定的计算机上登录需要单击“登录到”按钮,打开“登录工作站”对话框,如图 2-18 所示。

用户可以通过域控制器管理的任何计算机登录,也可被限制在指定的计算机上登录。在图 2-18 中选择“所有计算机”单选按钮,就是允许该账户可以通过任何计算机登录。但是在企业实际应用中,出于对特殊用户的安全要求,是不允许使用非本人使用的专用计算机或部门之外的计算机,因此特殊用户的登录地点就要被约束。例如,财务部门的用户不能随意使用网络中任何计算机,只能在财务办公室使用本部门计算机。可在“登录工作站”对话框中选中“下列计算机”单选按钮,在“计算机名”文本框中输入该账户要登录的计算机名称,然后单击“添加”按钮,这样该账户就只能通过指定计算机登录到域控制器管理的网络系统中。如果该用户需要从多台计算机登录时,可重复输入多台计算机的名称,如图 2-19 所示。



图 2-18 在指定计算机登录



图 2-19 账户从指定计算机登录设置

在指定的时间登录设置中,对登录域控制器的账户可以限制在一个特定的时间范围内。在“账户”选项卡中单击“登录时间”按钮,打开如图 2-20 所示对话框。在登录时间设

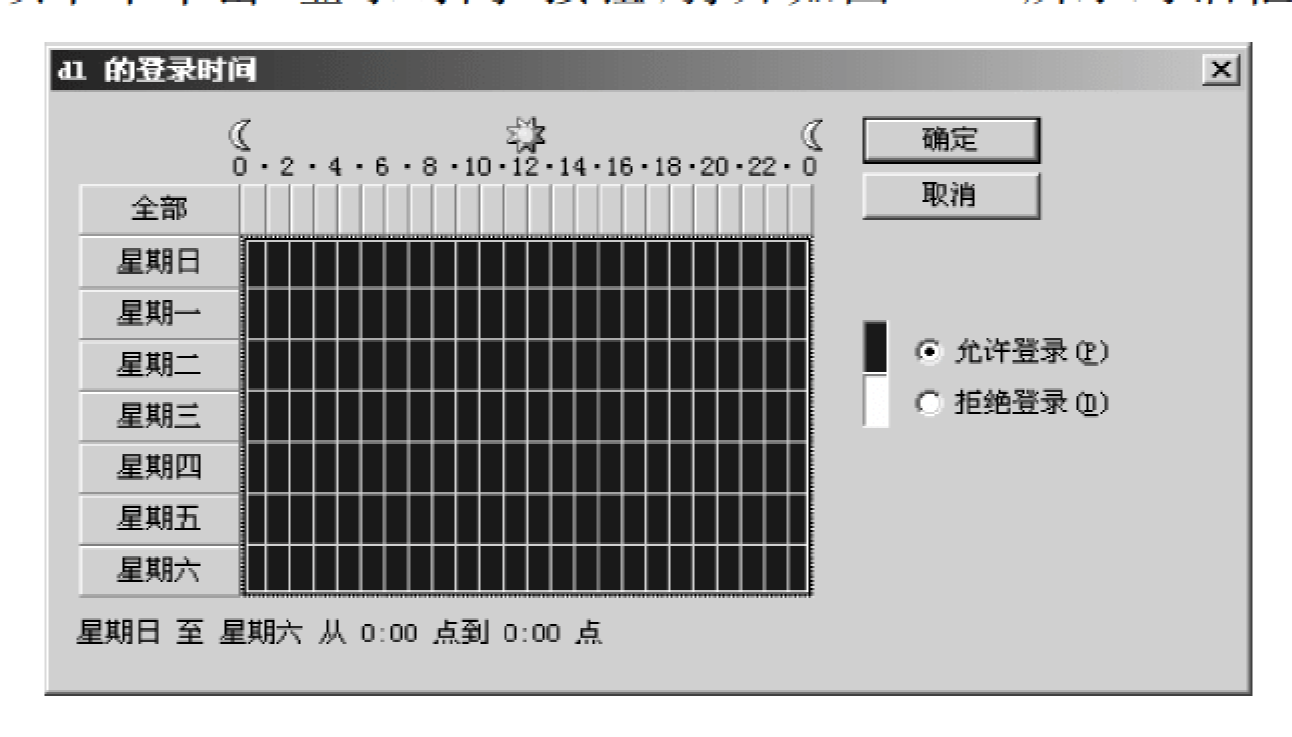
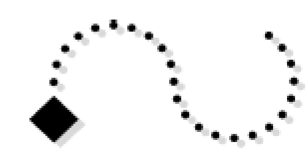


图 2-20 设置账户在指定时间登录



置对话框中可以设置指定的日期和指定的时间，单击“确定”按钮，让用户在一个规定的时间内登录域控制器。

例如，公司指定用户 DL 只能在上班时间使用计算机，上班时间为周一至周五的早 9 点至下午 6 点，可按照如图 2-21 所示设置登录时间。

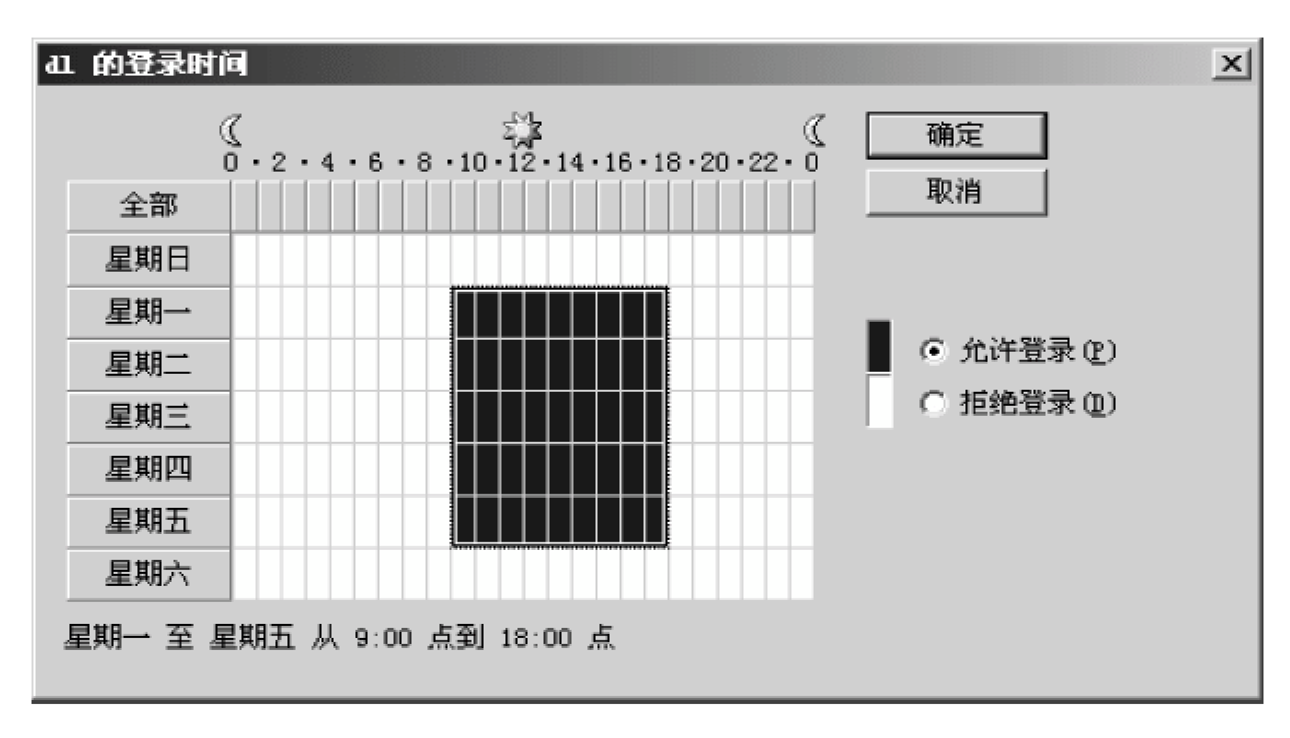


图 2-21　设置账户在指定时间登录域控制器计算机系统

③“账户选项”选项组提供多项有关账户安全方面的设置，在后面的课程学习后再就此展开实验，如图 2-22 所示。

④“账户过期”选项组对账户登录计算机的时间做出了更严格的限制，可以选择“永不过期”或“在这之后”单选按钮，指定具体的日期来限制该账户登录到域控制器中，这样，在此日期之后，该用户就不能登录到系统中了。

(2) 账户的删除

在日常的系统管理中，主要是对系统资源和账户的管理。在账户管理中经常出现原有创建的账户不使用的情况，主要有：实验用账户、误操作建立的账户、临时账户和禁用的账户。对于这些账户，一般情况下管理员可执行账户删除操作，将账户从域控制器中删除；但是在 Windows Server 2003 操作系统中，确认和识别账户不是用户表面上看到的账户名，而是在账户建立的开始系统为每个账户自动分配惟一一个安全标示(SID)。当一个账户不使用时，如果删除该账户，该账户的 SID 并没有作废，该账户在资源对象上设置的权限仍然存在。如果用户再新创建一个与已经删除的账户同名用户，在计算机系统内部则是不同的 SID，即拥有不同权限。因此作为账户管理者，只有在一个账户真正作废不用才有删除的必要，建议对暂时不使用的账户可以先禁用。

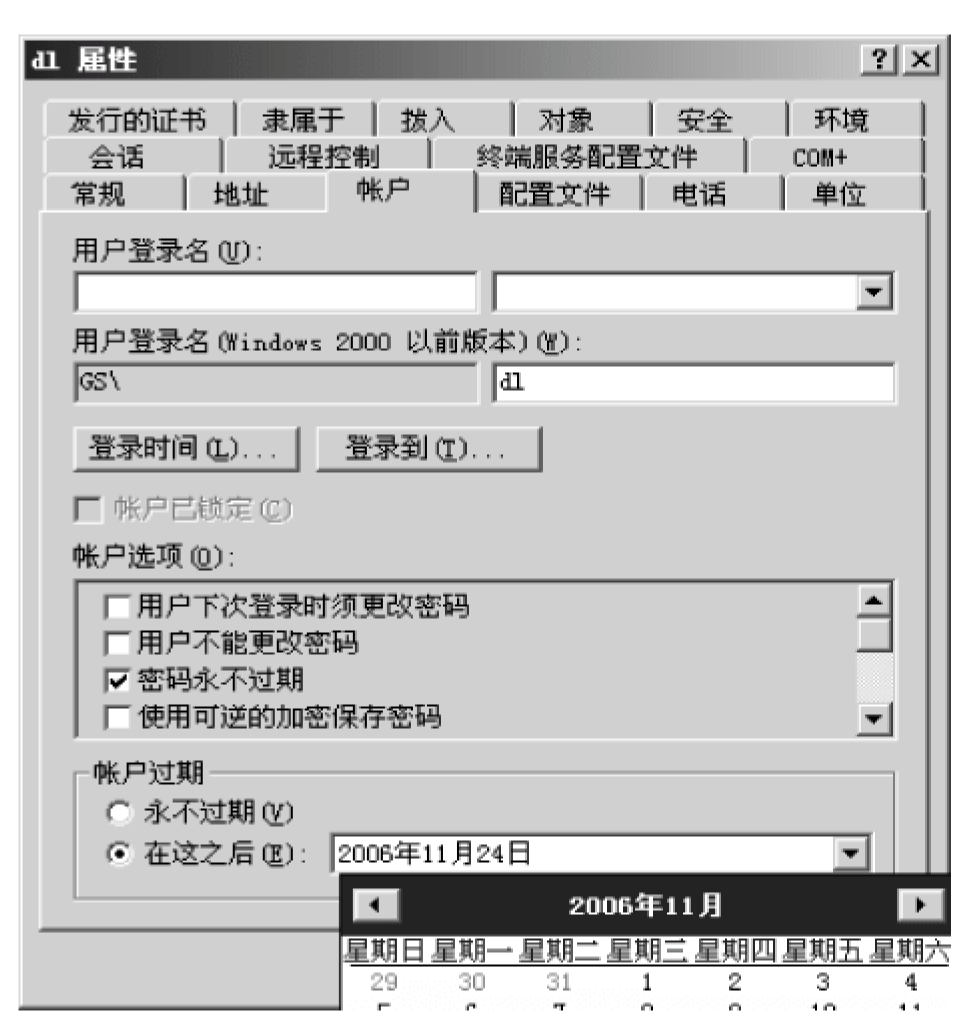
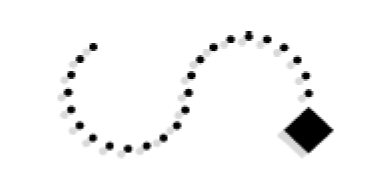


图 2-22　“账户选项”选项组



2.1.2 域模式下组的设置与管理

1. 域模式下组的概念

在 Windows Server 2003 的域控制器中，组是一个非常重要的概念与应用。在第 1 章已经就组的原理作了介绍。账号是进入系统的身份证，组是用来简化、统一管理账户的逻辑结构，利用组可以把具有相同权限需求和管理需求的用户组织放置在一个逻辑单元中，这样便于管理和提高工作效率。

(1) 组账号的特点

- 组是个逻辑结构。
- 一个账户可以同时加入多个组。
- 当一个用户加入到一个指定组时，该用户账号就拥有了该组所拥有的所有权限。

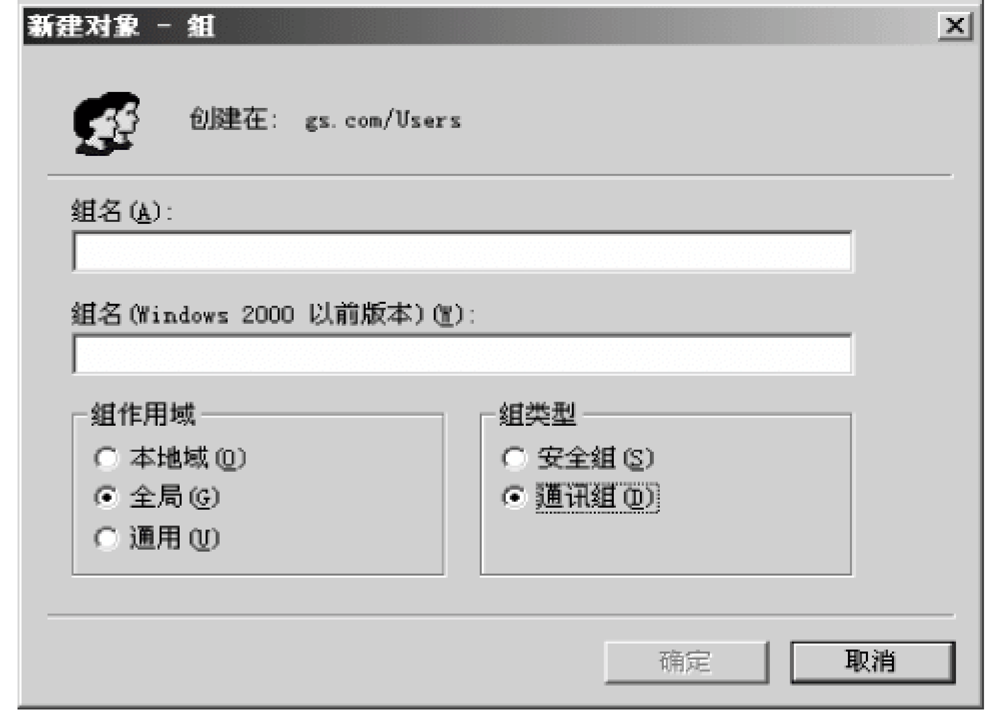
例如，当我们来到企业进行实习时，每位同学事先准备了不同颜色的帽子，领队通知大家，戴红色帽子的同学进左手门，戴黄色帽子的同学进右手门，这时在各个门口守卫的保安并不认识同学，可他会根据每个人所戴帽子颜色来判别是否允许进入。所以帽子赋予了每位同学相应的权利，帽子就是一种逻辑组。

(2) Windows Server 2003 组的分类

在 Windows Server 2003 中，因组的作用不同，建立了不同类型的组，组有两种类型：通信组和安全组。

通信组用来组织用户账号，没有安全性，在通信组中可以存储用户账号等信息，可用于微软的其他相关软件，如 Exchange 2003 Server。通信组如图 2-23 所示。

安全组除了通信组所具备的功能外，主要用于为用户和计算机设置权限。安全组是 Windows Server 2003 权限管理的重要组成部分，主要是对所包含的账户在资源对象中的访问进行控制。安全组如图 2-24 所示。



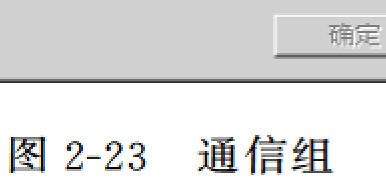


图 2-23 通信组



图 2-24 安全组

(3) Windows Server 2003 组的范围

组的范围是用来管理组的作用域的，在域中根据组的范围分为 3 种类型，即全局组、本地组和通用组。

全局组用来管理具有相同管理任务的用户账号，在该组中只能包括该组所在域的用户账户，该组可成为域的本地组的成员。

本地组与全局组不同，本地组的目的是给本域中的资源分配权限，本地组只在本域中可见。该组可以包括任何域的用户账号和任何域的全局组和通用组。

通用组具备了全局组和本地组的作用，其成员灵活，其作用主要是在多域模式下组织全局组。

（4）Windows Server 2003 中的默认组

在一个域搭建好后，打开“Active Directory 用户和计算机”窗口中的 Users 文件夹，就会显示一些已经存在的账户和组，如图 2-25 所示。

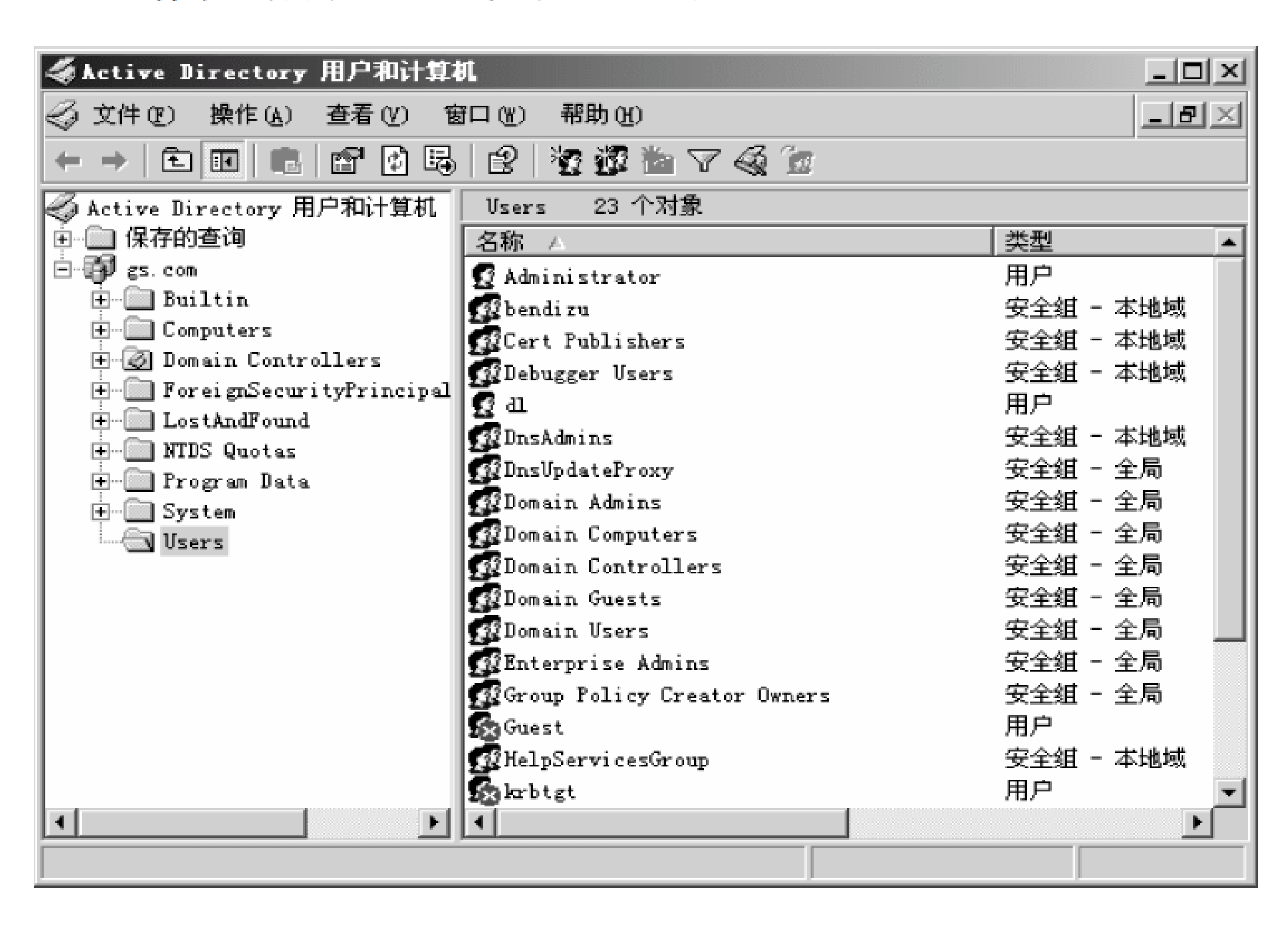


图 2-25　各个默认组

这些组可以分成预定义组、内置组、内置本地组和特殊组 4 类。

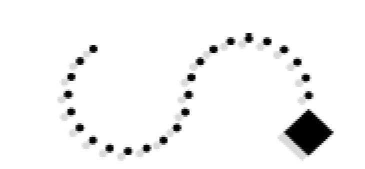
① 预定义组。这些组创建在 Users 文件夹中，默认情况下为全局组，没有任何继承权力。例如：

- Domain Admins(域管理员组)，自动将该组加入到 Administrators，具有域的管理权限。
- Domain Guests(域来宾组)，具体解释说明看文件夹中的“描述部分”。
- Domain Users(域用户组)，自动加入本地 Users 组中，成为域中用户组成员。

② 内置组。在 Builtin 文件夹中建立的组为内置组，如图 2-26 所示。

内置组都是安全本地组，提供预定义用户权力和权限的管理，这些组已经设置好相应的权限，如果让那些用户执行相应的管理权限时，只要把这个用户账号加入到对应组中即可。

- Account Operators(用户账户操作员组)：成员可以管理域用户和组账户，但不能修改 Administrators 组的任何信息。



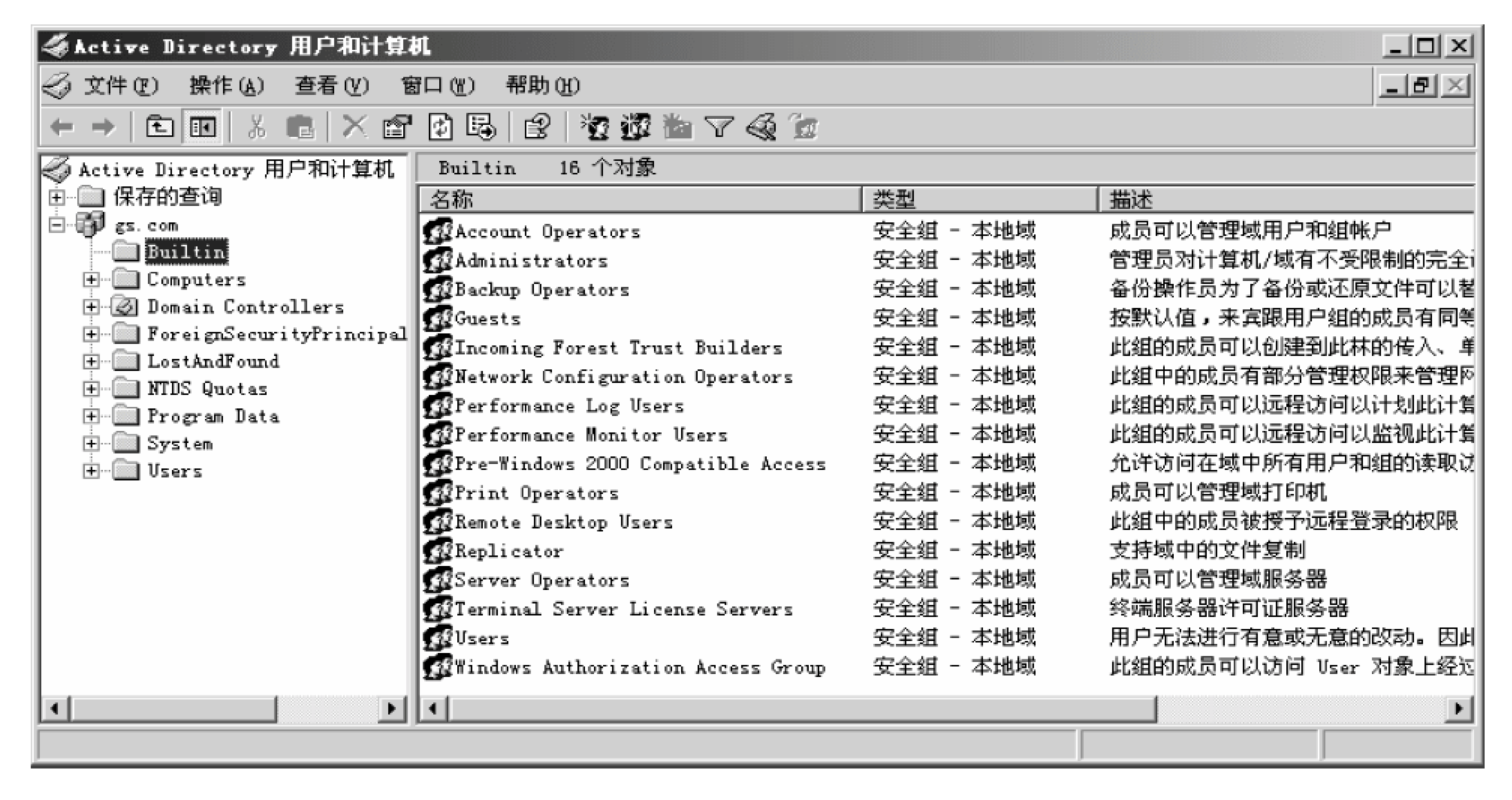


图 2-26 内置组

- Administrators(管理员组)：管理员对计算机/域有不受限制的完全访问权。
- Backup Operators(备份操作员组)：备份操作员为了备份或还原文件可以替代安全限制。
- Users(用户组)：用户无法进行有意或无意的改动，可以运行经过验证的应用程序，但不可以运行大多数旧版应用程序。

③ 内置本地组。该组不属于活动目录域模式下的组，前面已经讲述。

④ 特殊组。该组没有特定用户账户，但可以在不同时候代表不同用户。例如，Everyone(每人组)。

2. 组的设置

前边已经就组的有关概念进行了分析，在组的实际使用时，有关组的设置包括几个具体的工作，通过这些工作可以对组进行有效的维护。

(1) 组账号建立

域模式下组的建立与第 1 章介绍的组的建立基本相同，其具体操作如下：

① 右击“Active Directory 用户和计算机”窗口中 Users 文件夹，在弹出的快捷菜单中选择“新建”→“组”命令，如图 2-27 所示。

② 在“新建对象—组”对话框中输入相应的信息并设置组作用域、组类型，然后单击“确定”按钮，如图 2-28 所示。

(2) 设置组成员

使用组账户就是管理和组织用户账户，因此需要在建立的组中加入相应的用户账户。这个过程可以通过用户账户实现，也可通过组账户属性实现，具体操作如下：

① 打开要加入账户的指定组的属性对话框的“成员”选项卡，如图 2-29 所示。

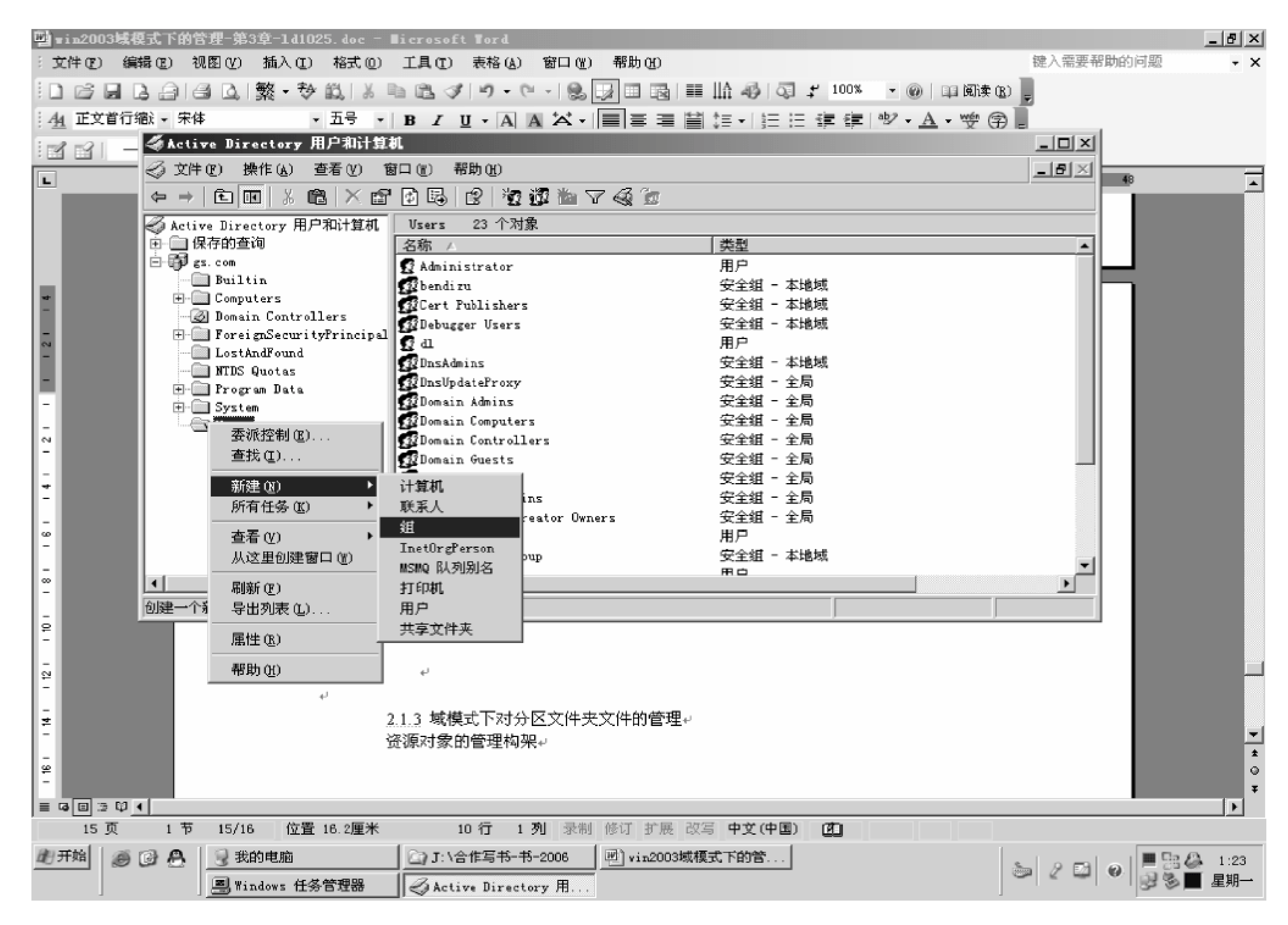


图 2-27 创建组



图 2-28 “新建对象—组”对话框



图 2-29 “成员”选项卡

② 单击“添加”→“高级”→“立即查找”按钮，显示被选用户账户，如图 2-30 所示。

③ 选中要加入组的用户账户，单击“确定”按钮，如图 2-31 和图 2-32 所示。

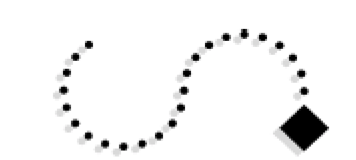




图 2-30 查找账户



图 2-31 选择账户



图 2-32 确定账户

④ 在“成员”选项卡中选择用户，然后单击“删除”按钮，可将指定用户从指定组中删除，如图 2-33 所示。

⑤ 打开要加入组账户的指定账户的属性对话框的“隶属于”选项卡，如图 2-34 所示。



图 2-33　删除账户

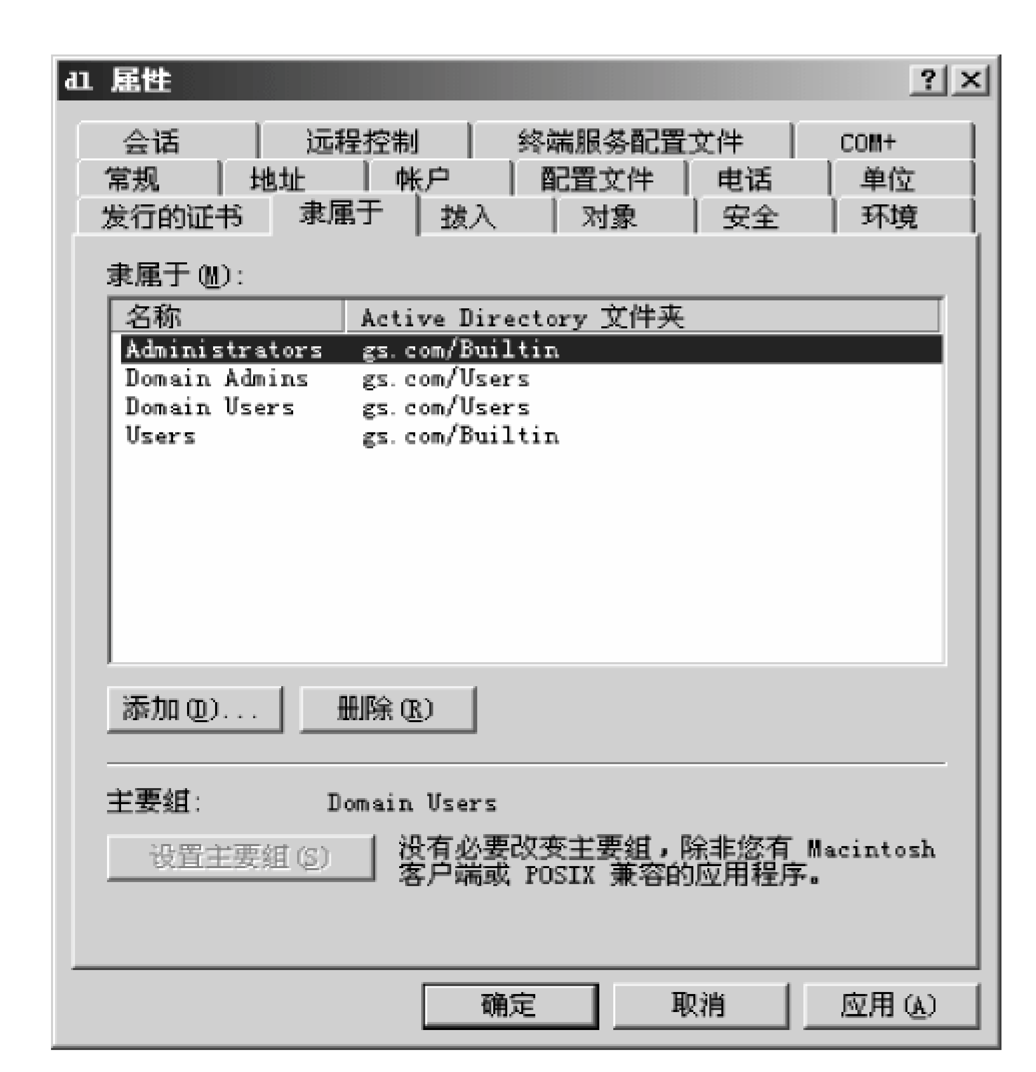


图 2-34　“隶属于”选项卡

⑥ 单击“添加”→“高级”→“立即查找”按钮，显示组账户，如图 2-35 所示。



图 2-35　组账户查找

⑦ 按照提示完成用户账户加入组的操作。

(3) 组的重命名

在建立好组账号后，往往因为各种原因要修改组名，这时，组中的成员不变，系统对组

的权限的设置与管理不会发生任何变化。在“Active Directory 用户和计算机”窗口中右击需要改名的组，在弹出的快捷菜单中选择“重命名”命令，如图 2-36 所示。

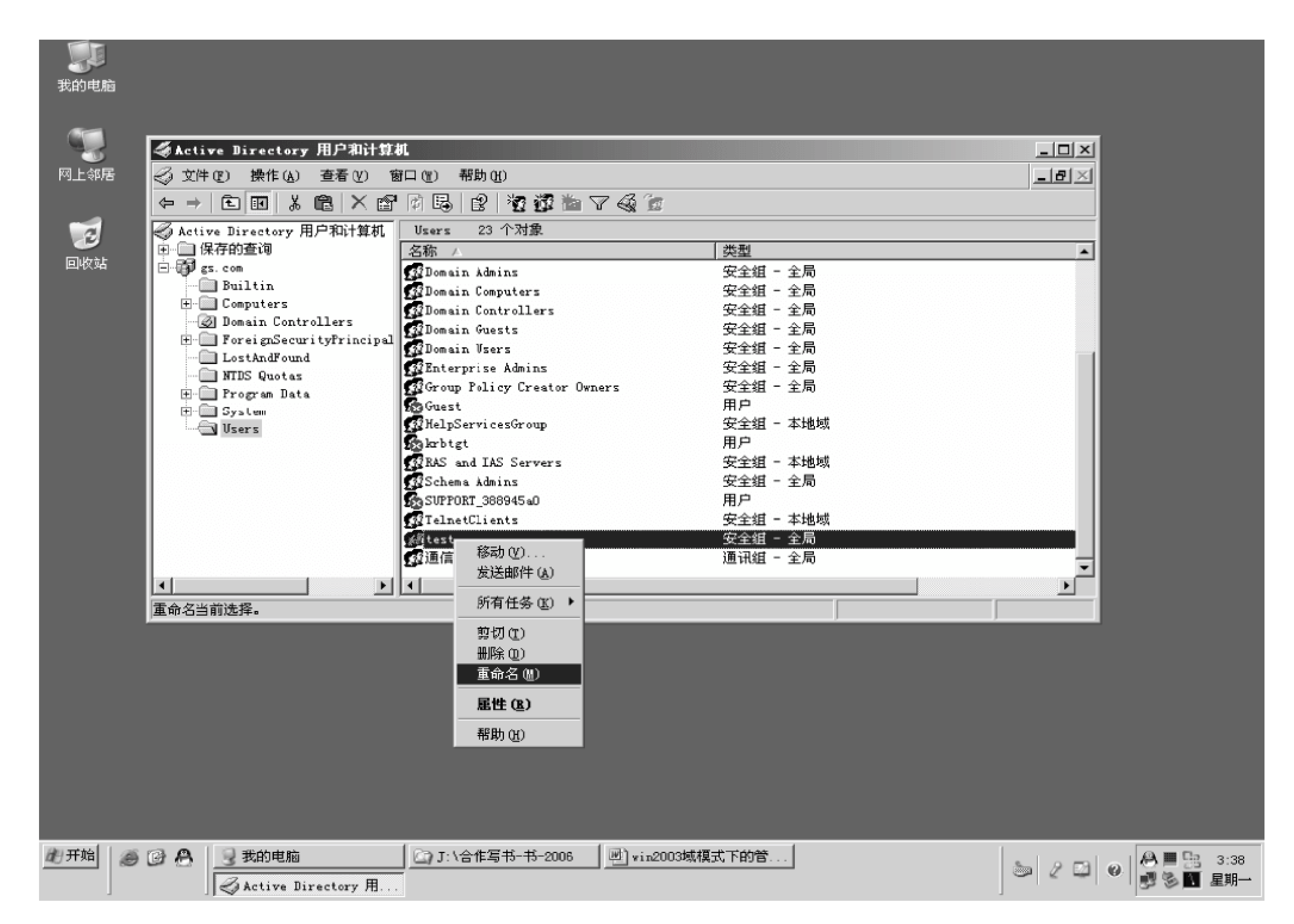


图 2-36 组名修改

（4）组的删除

当一个组需要删除时，可在“Active Directory 用户和计算机”窗口中右击要删除的组，在弹出的快捷菜单中选择“删除”命令，如图 2-37 所示。

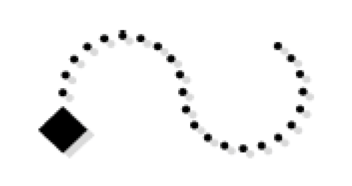
2.1.3 域模式下对分区文件夹文件的管理

1. 域模式规划与建立

在域模式下，一旦构架出符合需求的用户账户体系，确立了加入域的计算机后，最重要的工作就是确定哪些账户能访问哪些文件夹，对文件夹能进行什么权限的应用。这时候，用户账户已经成为域中一个成员，可以通过域中任何一台计算机登录，对任何计算机上的资源对象进行访问，如图 2-38 所示。

例如，现在有计算机 A、B、C，用户账户 H1、H2、H3，域名 GS.com。

① A 机为域控制器，B 机为客户机，C 机为客户机，域中计算机和账户构成如图 2-38 所示。



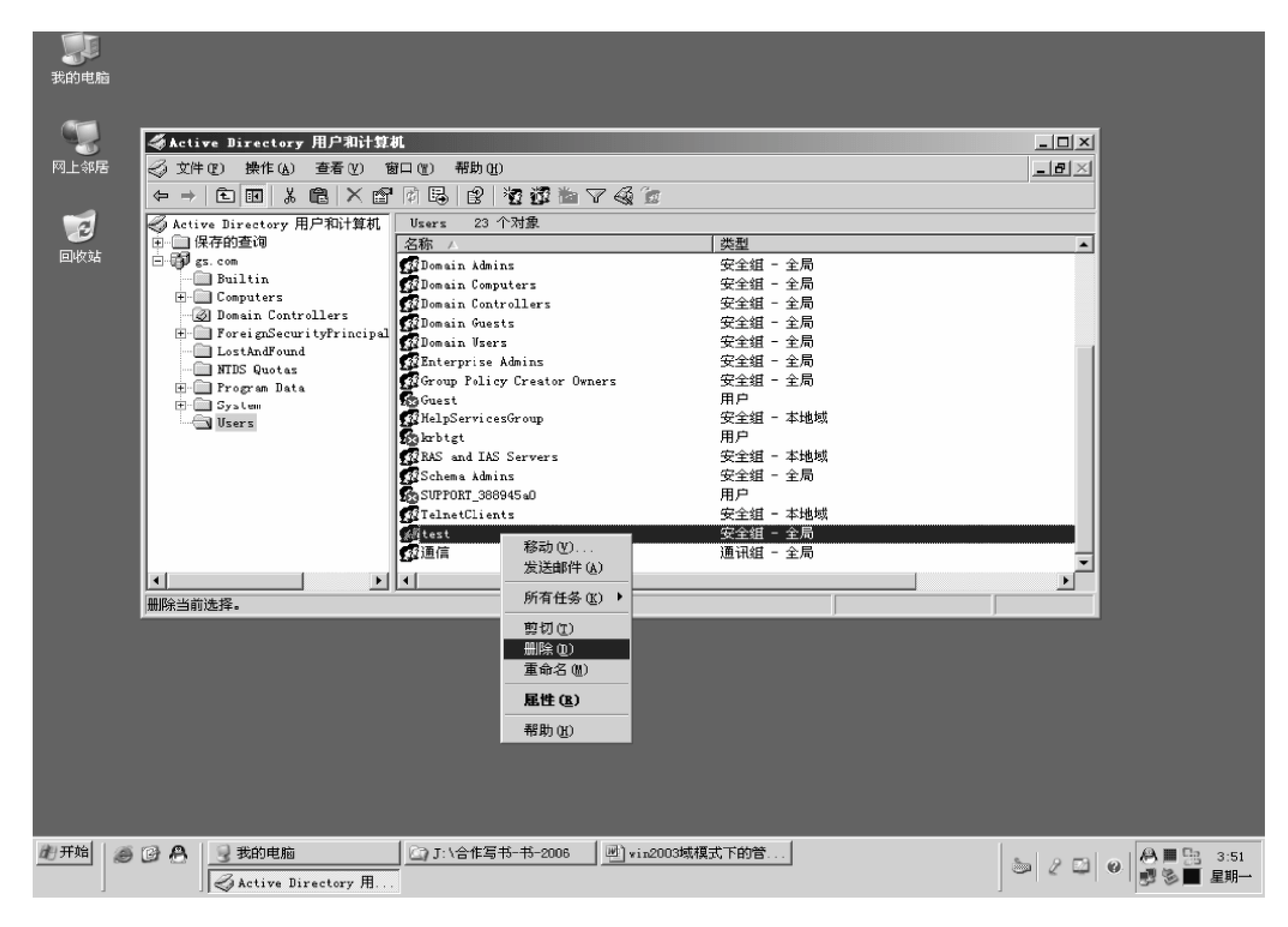


图 2-37 组的删除

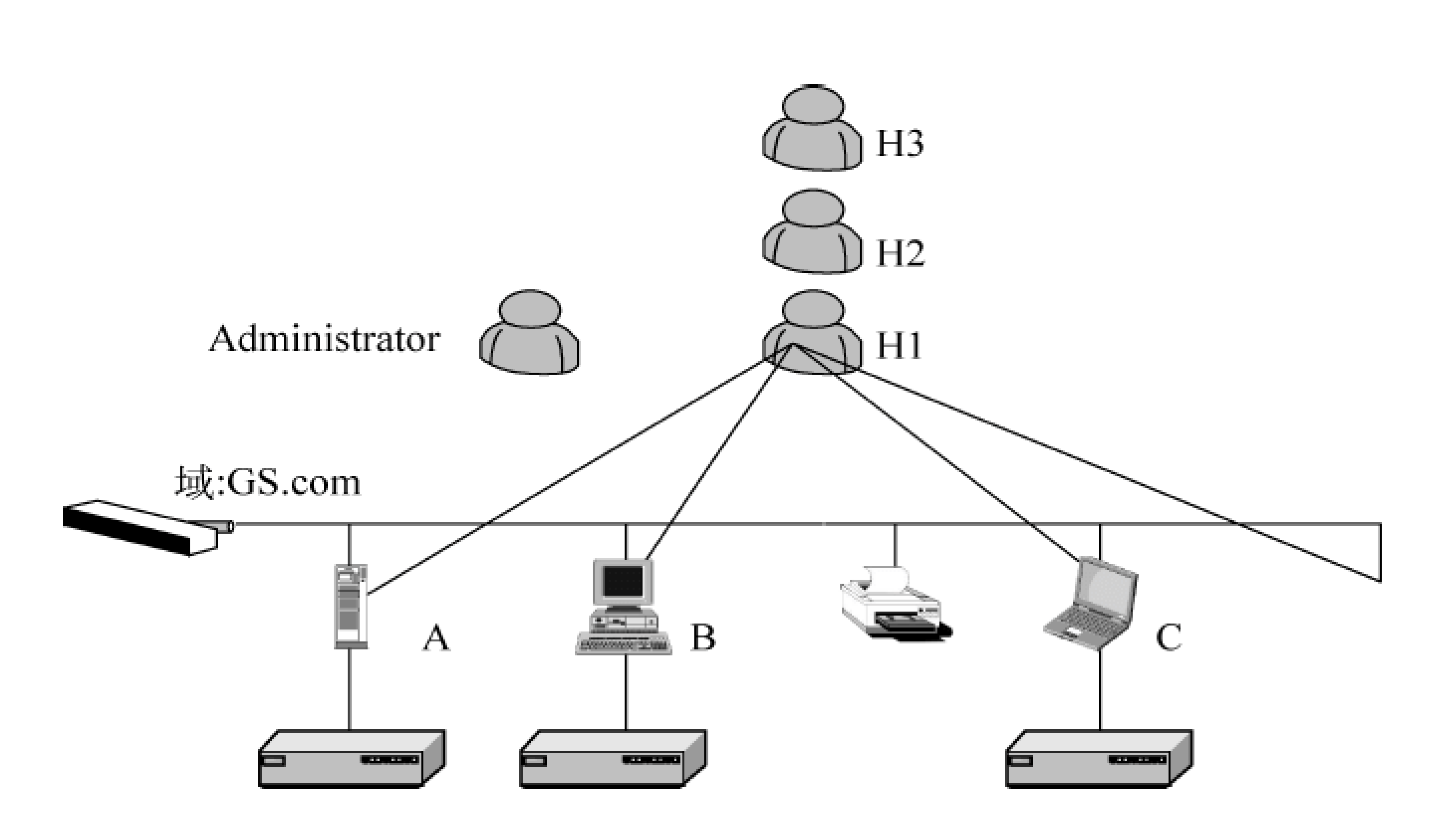


图 2-38 域中计算机和账户构成

② 将客户机 B 加入到 GS.com 域。在客户机 B 的桌面上右击“我的电脑”图标，选择“属性”命令，在“计算机名”选项卡中，单击“更改”按钮，如图 2-39 所示。在“隶属于”选项区中选中“域”单选按钮，在文本框中输入 GS.com。单击“确定”按钮，出现如图 2-40 所示

对话框。在用户名和密码文本框中输入管理员的用户名及密码。单击“确定”按钮，出现如图 2-41 所示对话框。重新启动计算机，使设置生效。



图 2-39　B 客户机加入到 GS. com 域



图 2-40　在 H1 加入 GS. com 域过程中输入账户 H1 密码



图 2-41　B 计算机称为 GS. com 客户机

采用相同的方法将计算机 C 加入 GS. com 域，这样构成了如图 2-38 所示的域模式。

2. 通过指定计算机登录对异地计算机的文件夹进行权限设置

H1 客户在 B 计算机登录，对计算机 C 上的文件夹 WH2 中的文件权限进行设置，如图 2-42 所示。这个过程不同于以前的过程，因为在计算机 C 没有成为 GS. com 的客户机时，对 C 机的文件夹权限设置必须在 C 机上进行；当 C 机成为客户机后，对域中所有的客户机的管理就变得方便了。

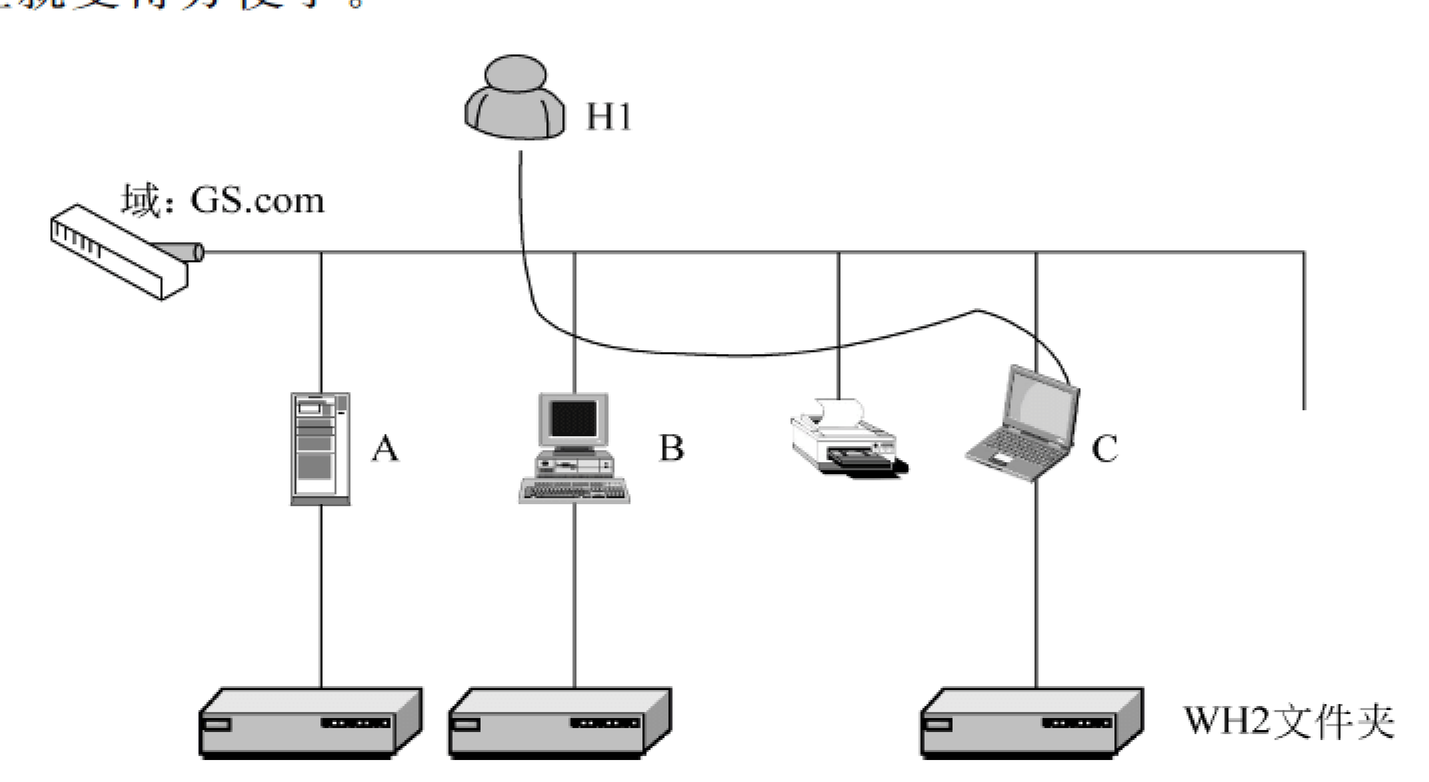


图 2-42　通过指定计算机登录对异地计算机的文件夹进行权限设置

2.2　设置组织单位与配置客户机

2.2.1　管理组织单位

1. 组织单位的概念的复习与使用

在2.1节已经就域模式下的计算机、账户的管理进行了分析与研究，通过域模式的管理体系可以使管理变得简洁高效。

但是在日常的网络操作系统中的管理还有着更加丰富和复杂的内容，例如，对账户使用计算机的系统配置的管理、对网络环境的管理、对桌面设置的管理、对安全设置的管理等。在这样的需求下，如果需要管理员为每个用户账户都一一进行设置，那将是个天文数字的工作量。

因此，应当通过一个适当的方法简化这些重复性工作。

在日常的企业工作中，公司人数众多，不可能一一管理，这时就要分析企业对员工管理的规律。通常企业是按照部门进行管理的，一个部门员工具有相同的工作环境、工作要求、相同的权利，这样就可以把员工的所有需求设置在一个属于部门的管理制度或管理方法中，当一个员工加入到该部门时，则所有的要求均依照部门要求执行。

在Windows Server 2003活动目录的域模式中，提供一个重要的功能——组织单位(OU)。它是非常重要的一个组件，在资源组织和管理上起着重要的作用，它可以将被管理的对象，统一放置在一个逻辑机构内，这些对象包括：用户账号、组账号、计算机、打印机、共享文件夹以及子OU。当这些对象被放置在OU容器中，围绕着这个OU就可以进行一系列的管理设置了。

2. 组织单位与组账号的区别

组织单位与组账号都是域模式下的管理对象，组织单元管理的对象更多些，而组账号只对用户账户在文件夹上的权限进行管理。

删除组账号，组账号所管理的用户账号的逻辑关系被打破，但用户账户本身不会消失。删除了OU，在OU中设置的信息、加入管理的对象将随之删除。

3. 组织单位与域的关联

域是操作系统对所有与之连接的计算机和登录计算机的用户账户的全面的管理，是建立在活动目录中的最全面完善的网络管理模式，用户访问计算机时需先登录域再进入组织单元。

组织单位是在域模式中存在的一个具体的逻辑管理方式，组织单位依存于域。

例如，一个企业由各种环境、各种设备、各类员工、各项工作构成，在这个企业周边筑起围墙，这个围墙就是域。围墙内的一切受到了保护，围墙内的一切有着自己的天地，可以相互协调相互帮助；围墙外面的一切受到限制，要想进入企业必须通过安检和授权。企业构架如图2-43所示。

在企业中每个人都有自己的分工，都有自己的职权范围，最重要的是每位员工都归属到一个部门，因为企业的管理模式、工作类别、权力范围都有对不同类别工作的规范性的

要求，因此企业需要建立各个专业部门，一般情况下有技术、人事、财务等部门。企业机构示意如图 2-44 所示。

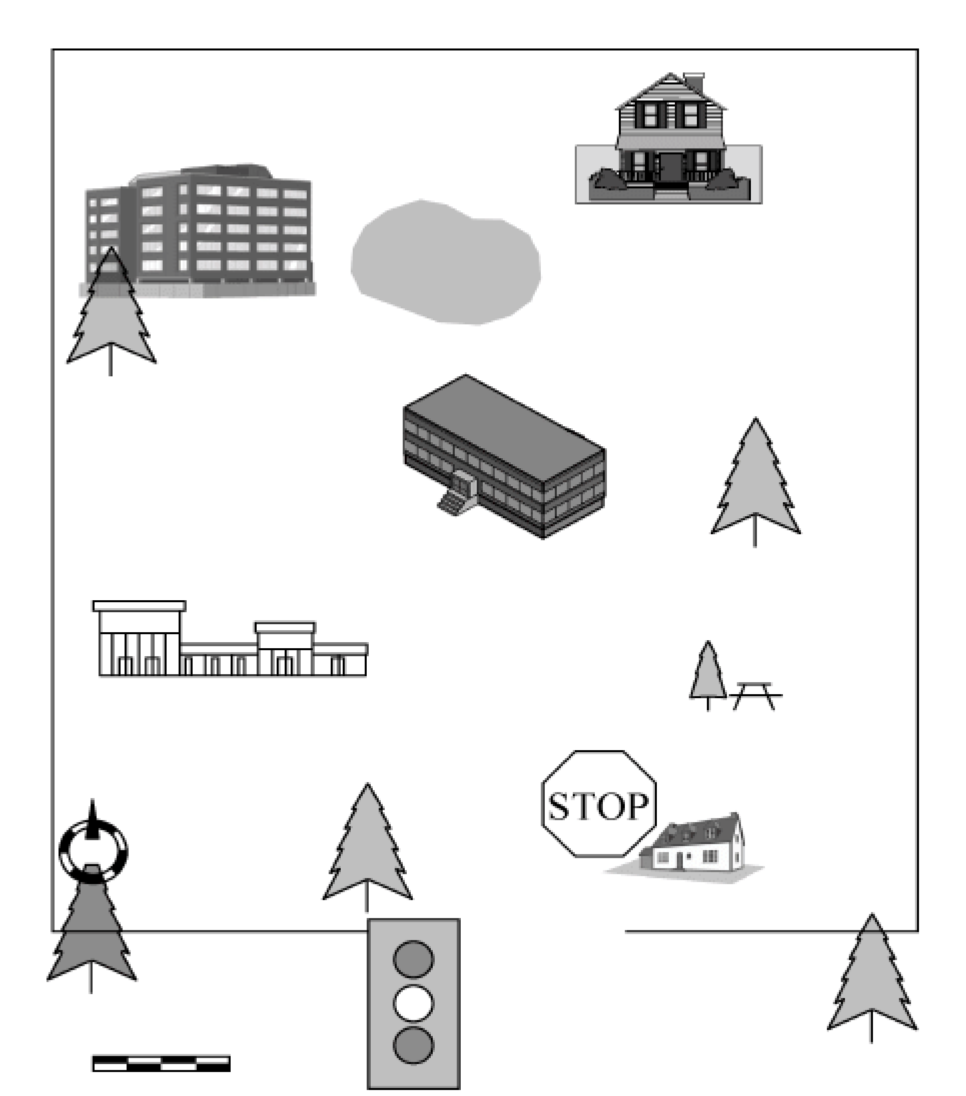



图 2-43　企业构架图

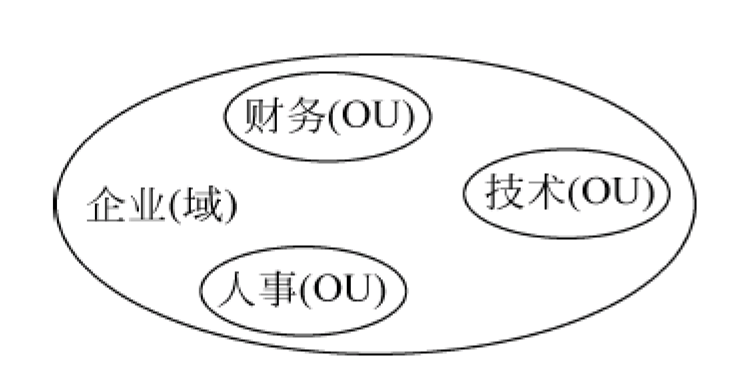


图 2-44　企业机构示意图

每一个部门有着一定的员工，有着该部门专用的设备，有着自己独特的管理方式，有着统一的着装，有着特殊的办公环境，有着独特的安全管理规定。

通过这个例子可以看出一个企业内部众多的员工被归属到各个部门，各个部门又有着自己的相对独立的管理方式。而这些独立的部门就是组织单位，各个部门的独立的管理规范就是组策略。

4. 创建组织单位

例如，要在 GS.com 域建立组织单位 caiwu，操作步骤如下：

(1) 在安装了活动目录的域控制器计算机上选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口，如图 2-45 所示。

(2) 右击 GS.com 域，在弹出的快捷菜单中选择“新建”→“组织单位”命令，如图 2-46 所示。

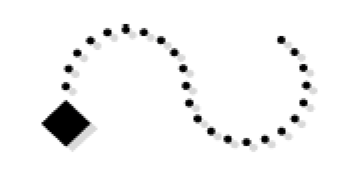
(3) 打开如图 2-47 所示的“新建对象—组织单位”对话框，并在“名称”文本框中输入 caiwu。

(4) 单击“确定”按钮，就建立了组织单位 caiwu。

2.2.2　配置客户机

本单元首先讲解将计算机加入域的方法，然后介绍通过活动目录对用户的计算机进行管理的方法。

例如，要将计算机 B 加入 GS.com 域(前提条件是网络的数据通信没有问题)。操作



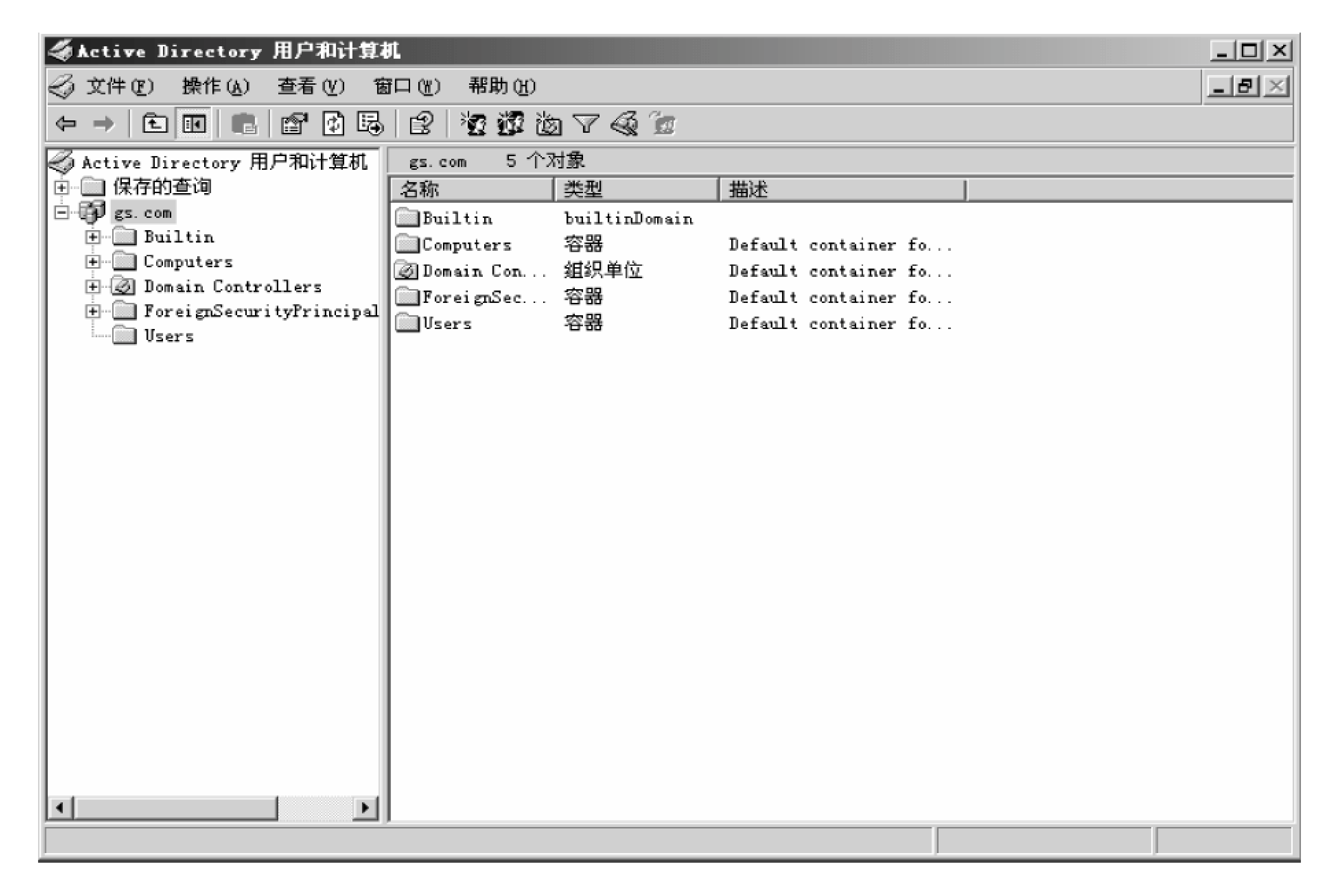


图 2-45 “Active Directory 用户和计算机”窗口

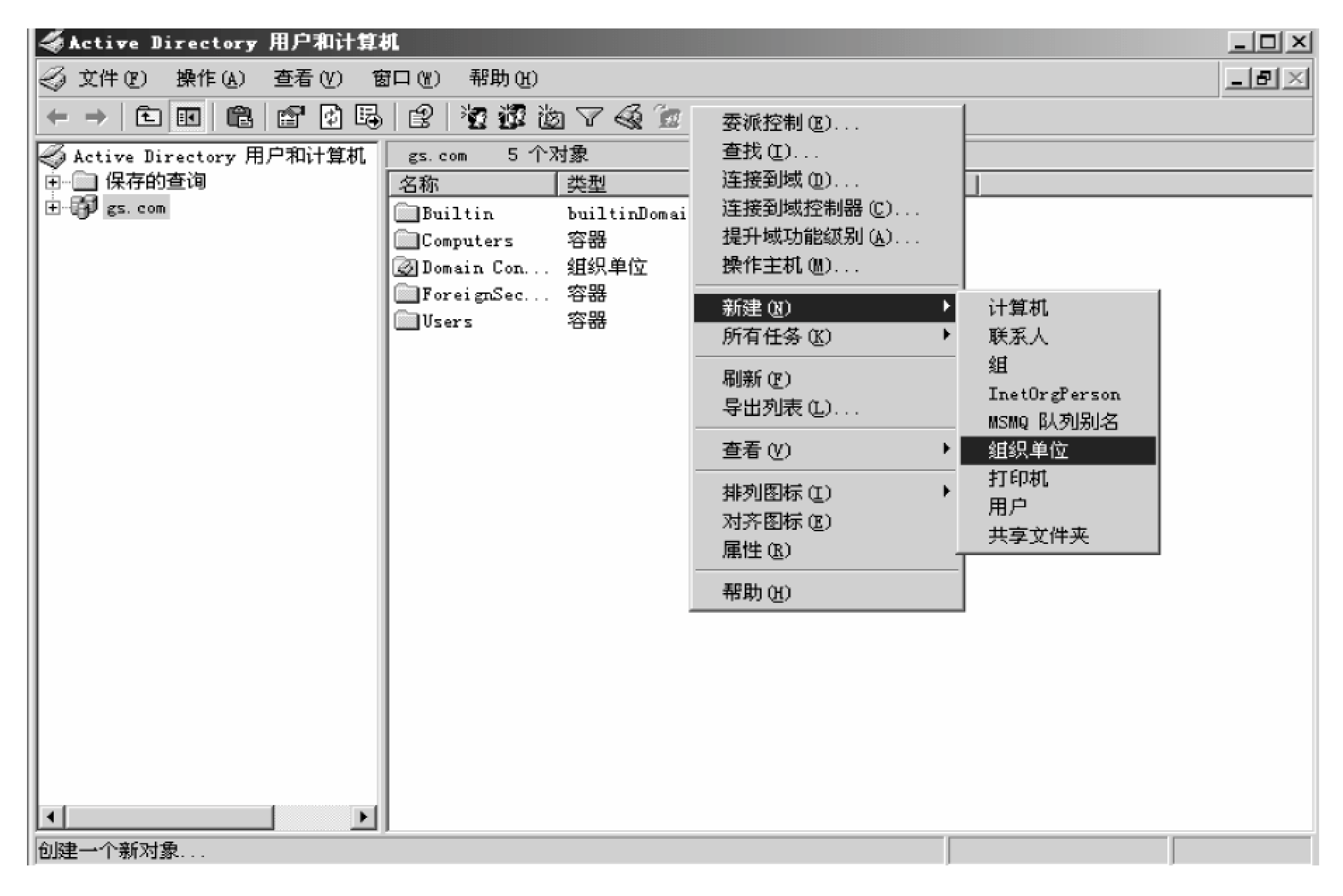
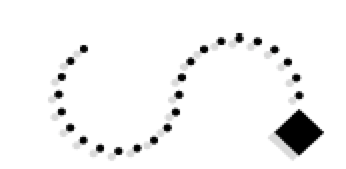


图 2-46 选择“新建”→“组织单位”命令



步骤如下：

（1）调整 TCP/IP 协议的属性，使 DNS 指向 GS.com 的 DNS(GS.com 的 IP 为 172.16.32.164)，如图 2-48 所示。



图 2-47　创建组织单位 caiwu



图 2-48　DNS 的调整

（2）右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，单击“计算机名”选项卡，如图 2-49 所示。

（3）单击“更改”按钮，打开“计算机名称更改”对话框，输入计算机名及要加入的域名，如图 2-50 所示。

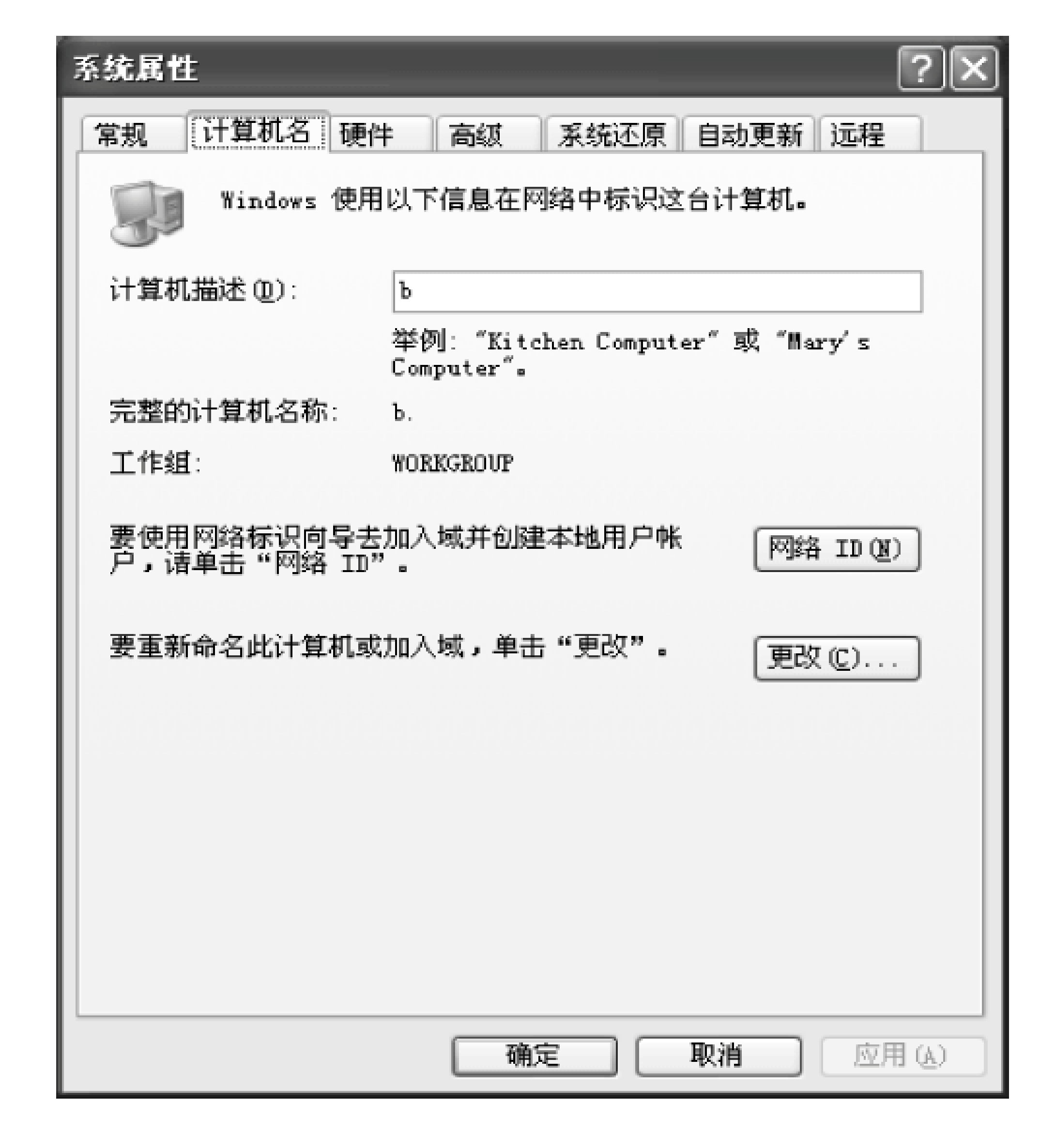


图 2-49　“计算机名”选项卡



图 2-50　更改操作

（4）单击"确定"按钮，打开如图 2-51 所示的"计算机名更改"对话框，输入有操作权的用户名及密码。

（5）单击"确定"按钮，弹出如图 2-52 所示的对话框，单击"确定"按钮。重新启动计算机，将计算机加入域的工作完成。

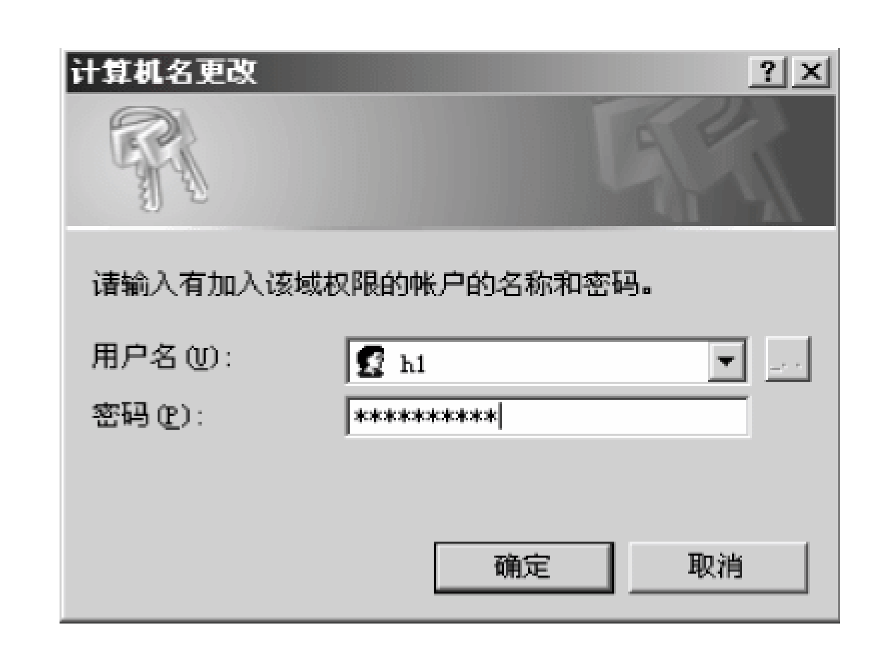


图 2-51　输入用户名及密码



图 2-52　将计算机加入域

将计算机加入域以后，就可以在域服务器上对加入域的计算机进行有效的管理。或在客户机上，通过"网上邻居"的活动目录项目对其他计算机或域服务器进行有效的管理。

假如 H1 是 GS.com 的管理员，现在他就可以对域内的计算机包括域服务器进行管理，这种管理是以管理员的身份登录后，在域内的任何一台计算机上进行的，不需要管理员亲自遍历每一台计算机，就像共享文件的访问权限管理一样，充分体现了域工作模式下集中管理的优点。域模式如图 2-53 所示。

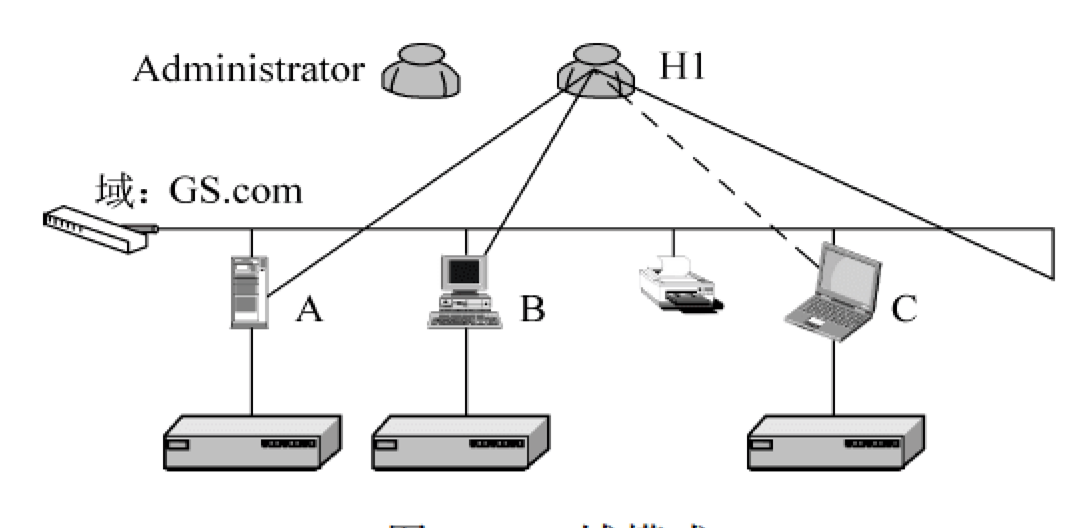


图 2-53　域模式

下面通过 GS.com 的域服务器观察域内计算机 B 硬盘文件分区状况。步骤如下：

（1）登录域服务器，选择"开始"→"程序"→"管理工具"→"Active Directory 用户和计算机"命令，打开"Active Directory 用户和计算机"窗口，如图 2-54 所示。

（2）打开 gs.com 下的 Computers 文件夹，右击计算机 B，在弹出的快捷菜单中选择"管理"命令，如图 2-55 所示。

（3）打开"计算机管理"窗口，如图 2-56 所示，就可对计算机 B 硬盘系统文件进行观察。

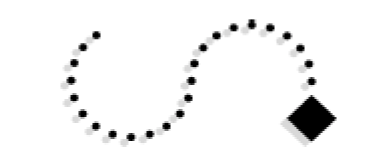






图 2-54　“Active Directory 用户和计算机”窗口

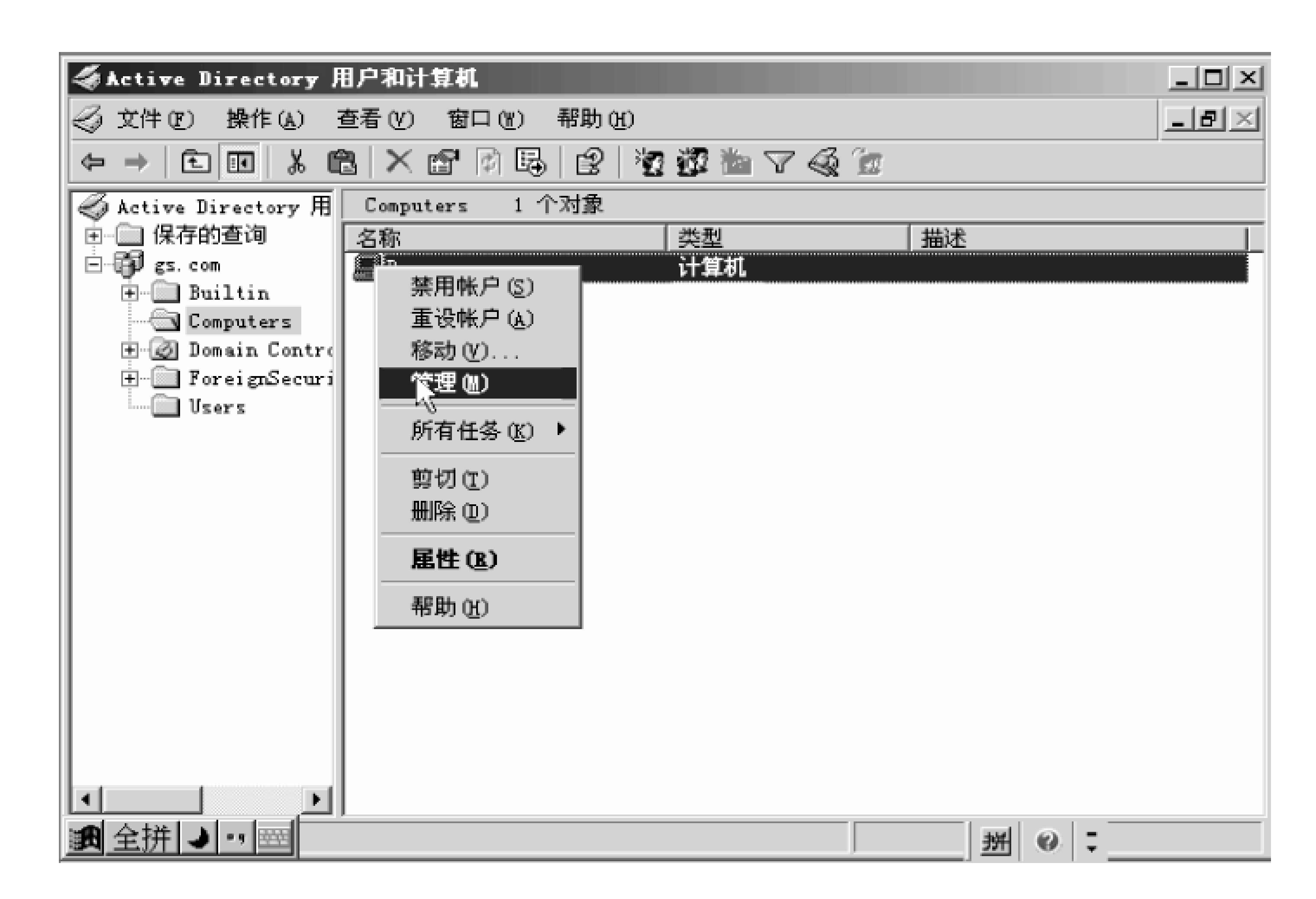


图 2-55　选择“管理”命令



图 2-56　计算机 B 文件系统

2.3 组策略

2.3.1 组策略的概念

1. 组策略的功能

注册表是 Windows 系统中保存系统、应用软件配置的数据库，随着 Windows 功能越来越丰富，注册表里的配置项目也越来越多。很多配置都是可以自定义设置的，但这些配置分布在注册表的各个角落，手工配置是相当困难和繁杂的。而组策略则将系统重要的配置功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理计算机的目的。组策略使用完善的管理组织方法，对各种对象中的设置进行管理，远比手工修改注册表方便、灵活，功能也更加强大。

通俗一点说，组策略是介于控制面板和注册表之间的一种修改系统、设置程序的工具。微软自 Windows NT 4.0 开始便采用了组策略这一机制，经过 Windows 2000 发展到 Windows 2003 已相当完善。利用组策略可以修改 Windows 的桌面、“开始”菜单、登录方式、组件、网络及 IE 浏览器等许多设置。

一些常用的系统、外观、网络设置等可通过控制面板修改，但大家对此肯定都有不满意，因为通过控制面板能修改的东西太少；水平稍高点的用户进而使用修改注册表的方法来设置，但注册表涉及内容又太多，修改起来也不方便。组策略正好介于二者之间，涉及的内容比控制面板多，安全性和控制面板一样非常高，而条理性、可操作性则比注册表强。

2. 编辑工具

如果是 Windows 2003 系统，那么系统已经默认安装了组策略编辑程序，选择“开始”→“运行”命令，在“运行”对话框中输入 gpedit.msc 命令，并单击“确定”按钮，即可运行程序。

使用上面的方法，打开的组策略对象就是当前的计算机。而如果需要配置其他的计算机组策略对象，则需要将组策略作为独立的控制台管理程序来打开，具体步骤如下：

(1) 打开 Microsoft 管理“控制台”窗口(可在“运行”对话框中直接输入 MMC 命令，就可运行控制台程序)，如图 2-57 所示。

(2) 在图 2-57 中单击“文件”→“添加/删除管理单元”命令，如图 2-58 所示。

(3) 在弹出的“添加/删除管理单元”对话框的“独立”选项卡中，单击“添加”按钮，如图 2-59 所示。

(4) 在“添加独立管理单元”对话框中，选择“组策略对象编辑器”，单击“添加”按钮，如图 2-60 所示。

(5) 在“选择组策略对象”对话框中，选择“组策略对象”为“本地计算机”，编辑本地计算机对象；或单击“浏览”按钮查找所需的组策略对象，如图 2-61 和图 2-62 所示。

(6) 单击“完成”按钮，然后单击“关闭”按钮，最后单击“确定”按钮，组策略管理单元就打开要编辑的组策略对象，如图 2-63 所示。



图 2-57 “控制台”窗口



图 2-58 文件菜单的使用

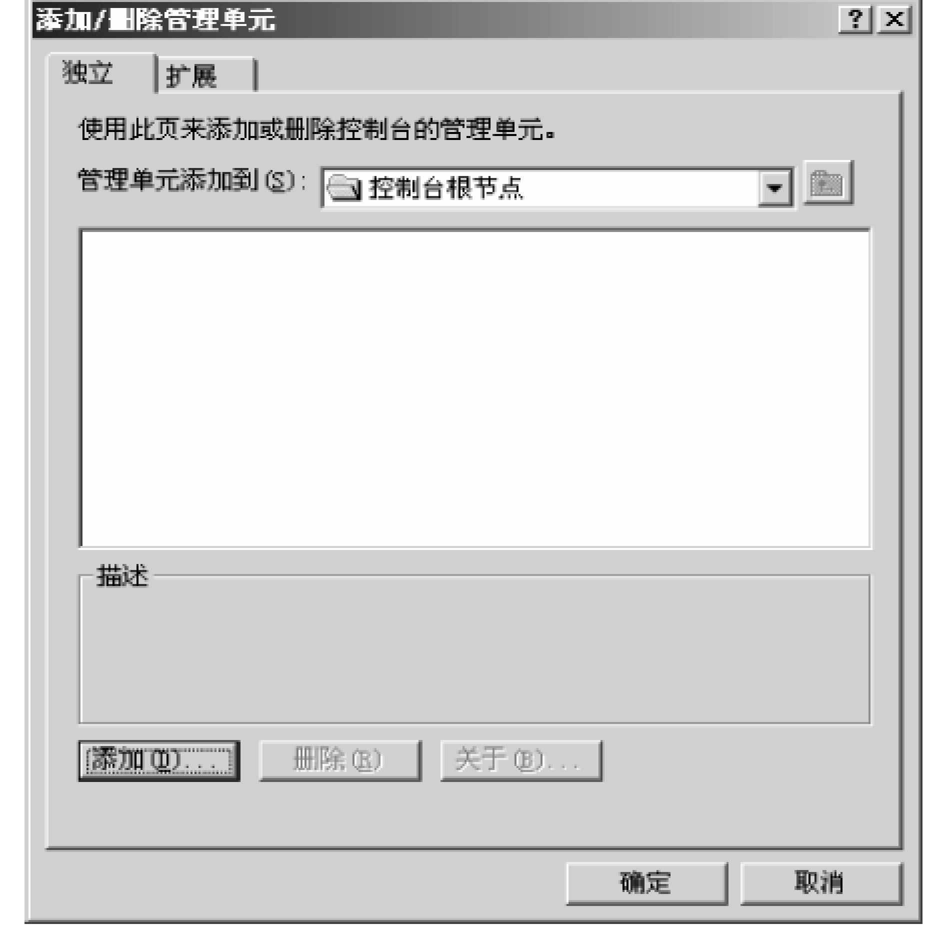


图 2-59 “添加/删除管理单元”对话框



图 2-60 “添加独立管理单元”对话框

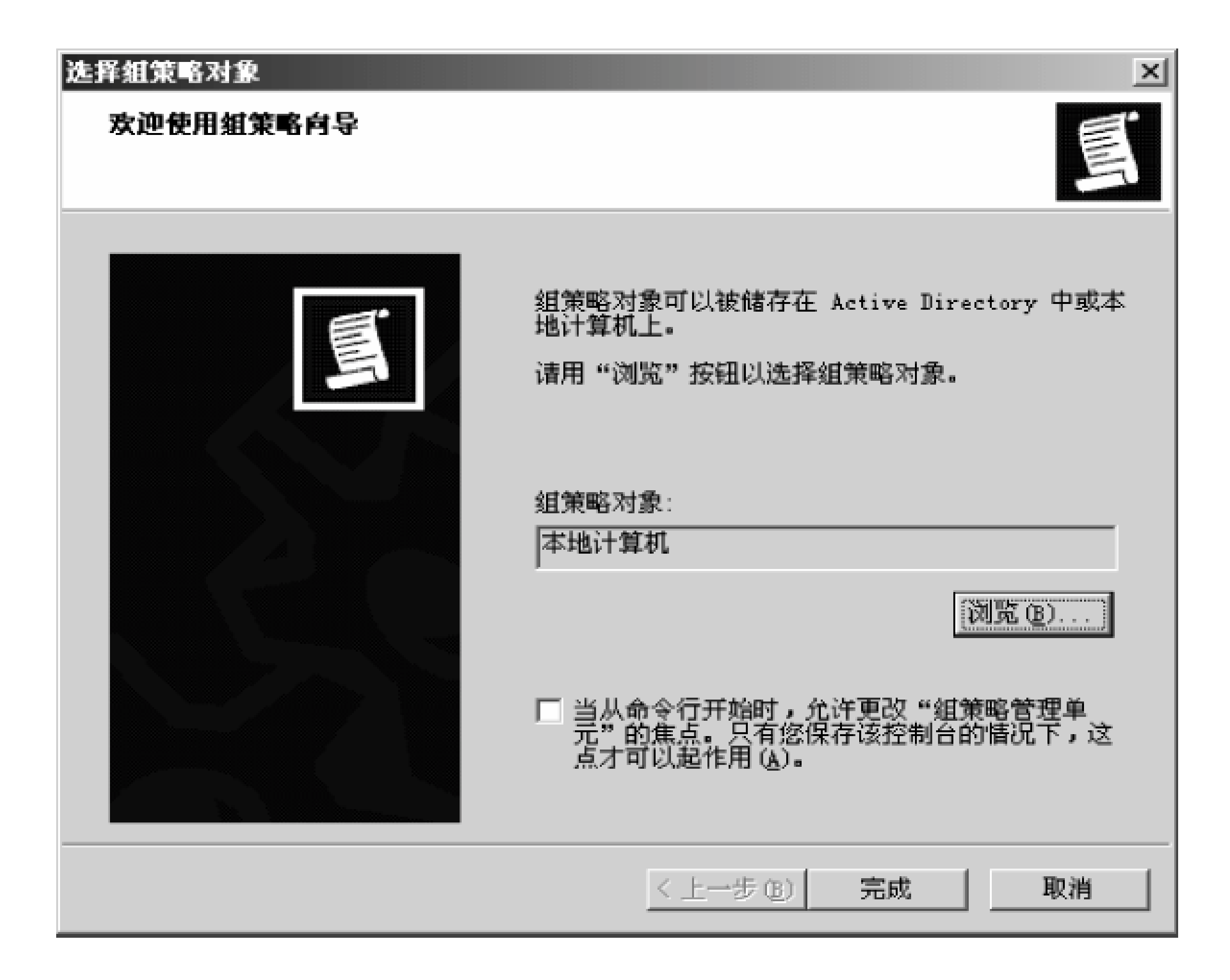


图 2-61　本地组策略

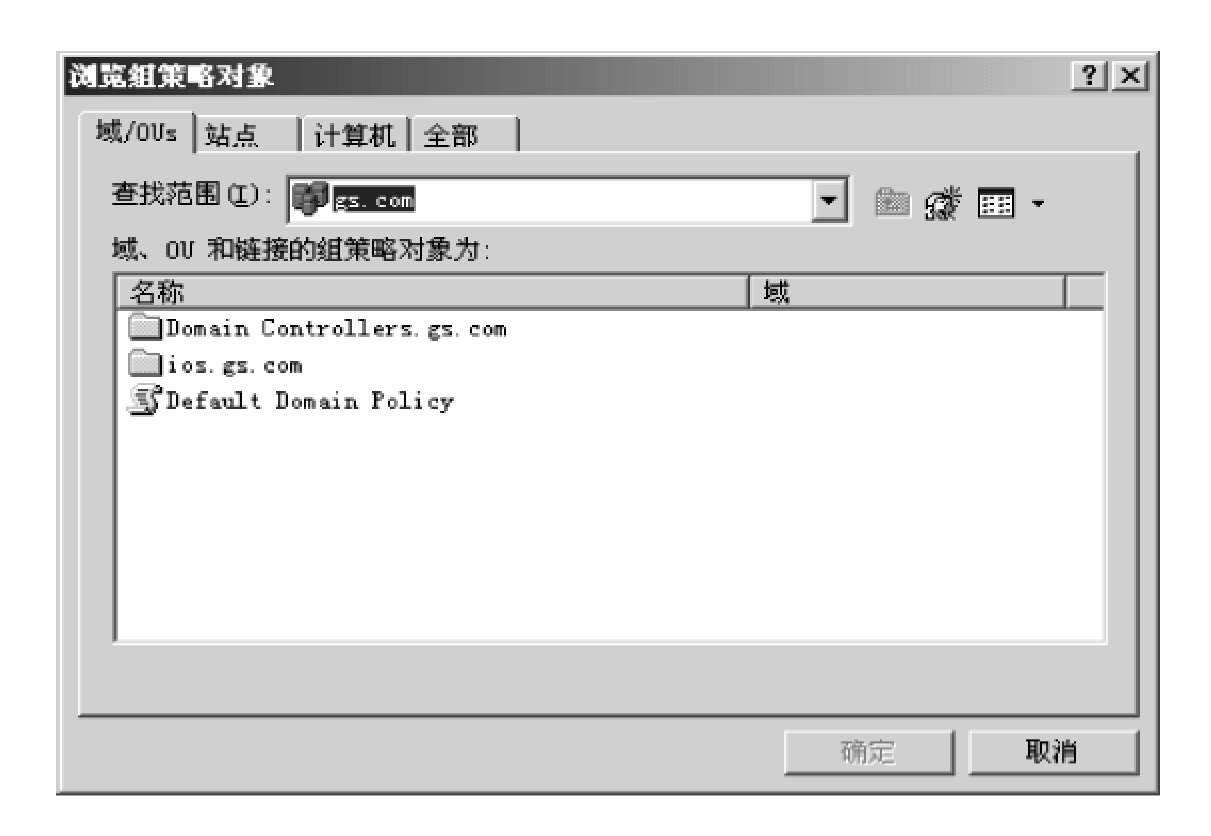
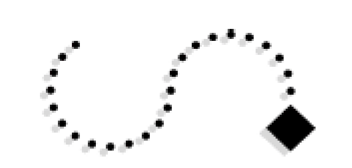


图 2-62　浏览域内的其他组策略



图 2-63　组策略界面



对于不包含域的计算机系统来说，在图 2-62 所示的对话框中，只有“计算机”选项卡，而没有其他选项卡。

通过上面的方法，就可以使用 Windows 2003 组策略系统强大的网络配置功能，让管理员的工作更轻松和高效。

2.3.2　组策略的内容

计算机组策略主要可进行两个方面的配置：计算机配置和用户配置。计算机配置是对整个计算机中的系统配置进行设置，它对当前计算机中所有用户的运行环境都起作用；用户配置则是对当前用户的系统配置进行设置，它仅对当前用户起作用。计算机配置和用户配置都提供了停用自动播放功能，但效果是不同的：如果是在计算机配置中选择了该功能，那么所有用户的光盘自动运行功能都会失效；如果是在用户配置中选择了该功能，那么仅仅是该用户的光盘自动运行功能失效，其他用户则不受影响。

当计算机配置与用户配置发生矛盾时，计算机配置优先，其下所有设置项的配置都将保存到注册表的相关项目中。计算机配置保存到注册表的 HKEY_LOCAL_MACHINE 子树中，用户配置保存到 HKEY_CURRENT_USER 子树中。在 Windows 2003 中，组策略一般放在“系统安装：\Windows\System32\GroupPolicy”文件夹中，文件名为 gpedit. msc。

“计算机配置”和“用户配置”中还有 3 个项目，如图 2-64 所示。



图 2-64　组策略对象

- 软件设置：用于对已经安装好的软件进行管理和维护。
- Windows 设置：用于系统或用户的开关机脚本和系统安全等内容的设置。
- 管理模板：主要用于对系统、网络、Windows 组件等内容进行设置，还可以添加或者删除管理模块。

2.4 利用组策略进行管理

组策略是 Windows 2003 中提供的一种重要的更新和配置管理技术。组策略与域或组织单位结合，就能控制和管理网络中域用户和计算机的工作环境。组策略有几百项配置，主要包括如下功能：用户工作环境的设置、安全设置、软件的安装与删除、脚本的设置、文件夹重定向。

2.4.1 创建和链接组策略对象

组策略设置存储在组策略对象（GPO）中，即组策略是由具体的组策略对象来实现的。根据组策略对象的作用范围，可分为两种类型。

（1）Active Directory 组策略对象存储在控制器上，只能在活动目录环境下使用，适用于组策略所作用的站点、域、组织机构中的用户和计算机。

（2）本地组策略对象只存在一台计算机上，只对本地用户及该计算机起作用。

当多个组策略在一起时，执行的顺序是本地组策略、活动目录的站点策略、活动目录的域策略、活动目录的组织单位策略。当这些策略不一致时，后应用的策略覆盖前一个策略。在活动目录层次结构的每一级组织单位中，可以链接一个、多个或不链接组策略对象。如果一个组织对象链接了多个组策略，则按管理员制定的顺序处理，较前位置的组策略具有较高的优先权。

下面介绍如何建立组策略和链接组策略。

1. 建立组策略

例如，要在 gs.com 域中建一个组织单位 is，并为之建立一个组策略。操作步骤如下：

（1）选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口，如图 2-65 所示。

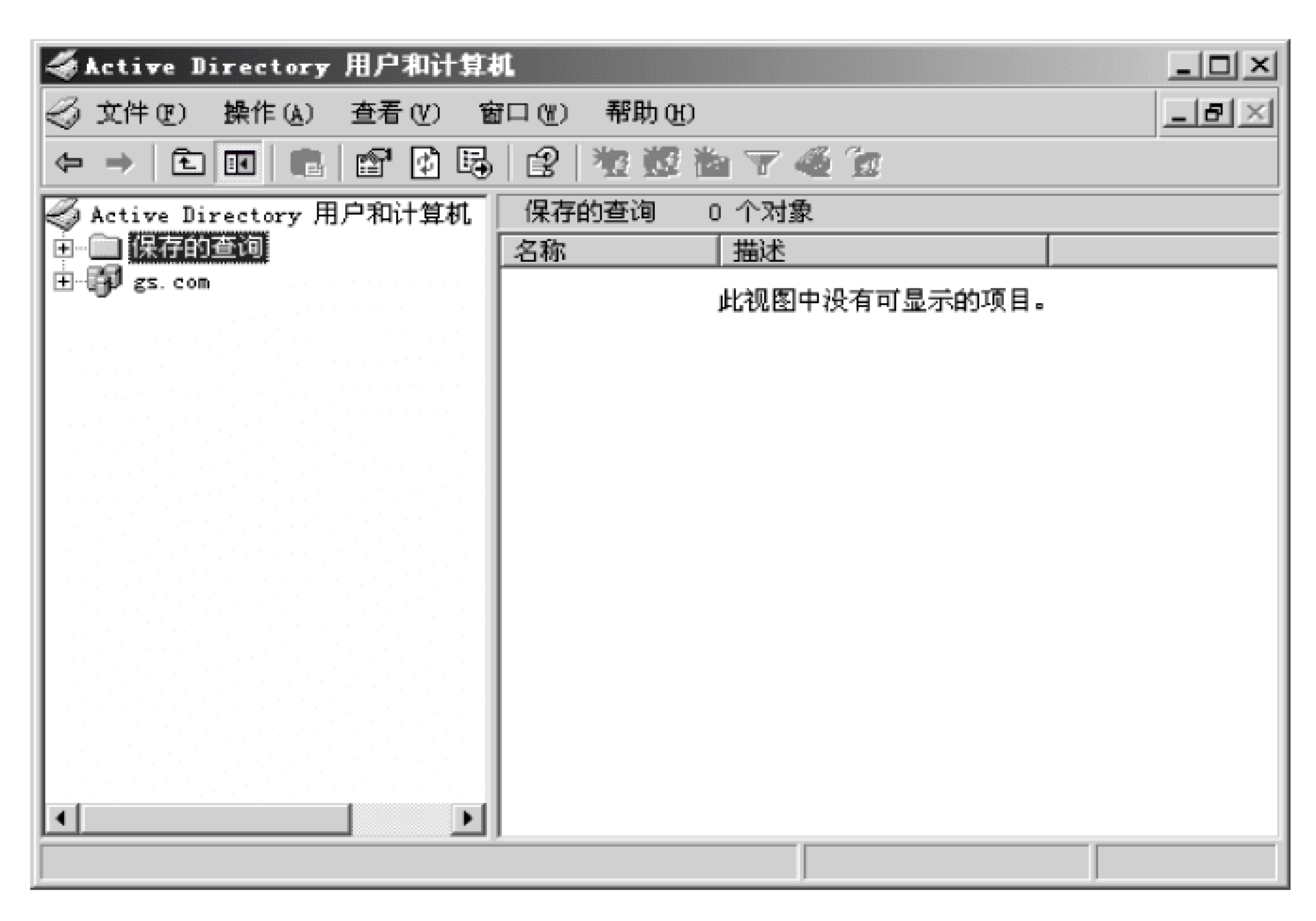


图 2-65 “Active Directory 用户和计算机”窗口

（2）选定 gs.com，在工作区右击，在弹出的快捷菜单中选择“新建”命令，并在对话框中输入 is，创建组织单位 is，如图 2-66 所示。

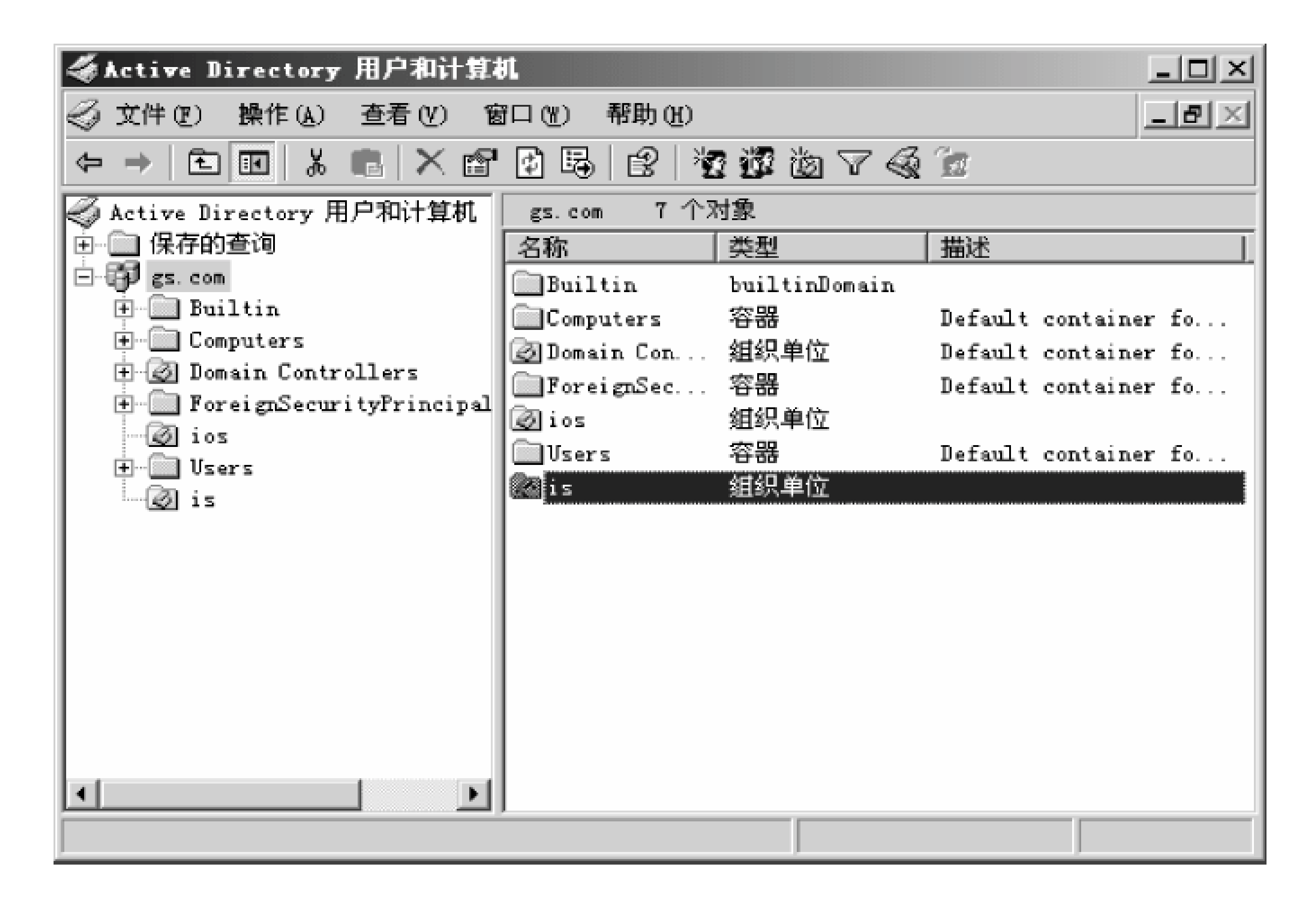


图 2-66　新建组织单位 is

（3）右击 is，在弹出的快捷菜单中选择“属性”命令，如图 2-67 所示。



图 2-67　组织单位 is 的快捷菜单

（4）在“is 属性”对话框中单击“组策略”标签，打开“组策略”选项卡，如图 2-68 所示。

（5）单击“新建”按钮，在对话框中输入组策略对象的名称 is，并选中 is 组策略对象，如图 2-69 所示。

（6）单击“编辑”按钮，在“组策略编辑器”窗口中对它进行编辑，如图 2-70 所示。



图 2-68 “is 属性”对话框



图 2-69 新建的 is 组策略对象



图 2-70 “组策略编辑器”窗口



图 2-71 “is 属性”对话框

2. 链接组策略

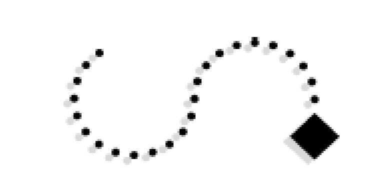
下面介绍如何进行组策略对象的链接。例如，将 ios 的组策略对象链接到 is 上，操作步骤如下：

（1）打开“is 属性”对话框，选中“组策略”选项卡，如图 2-71 所示。

（2）单击“添加”按钮，在“添加组策略对象链接”对话框中打开“全部”选项卡，如图 2-72 所示。

（3）选择 ios，单击“应用”按钮，如图 2-73 所示。

这时就将组织单位 ios 的组策略对象链接



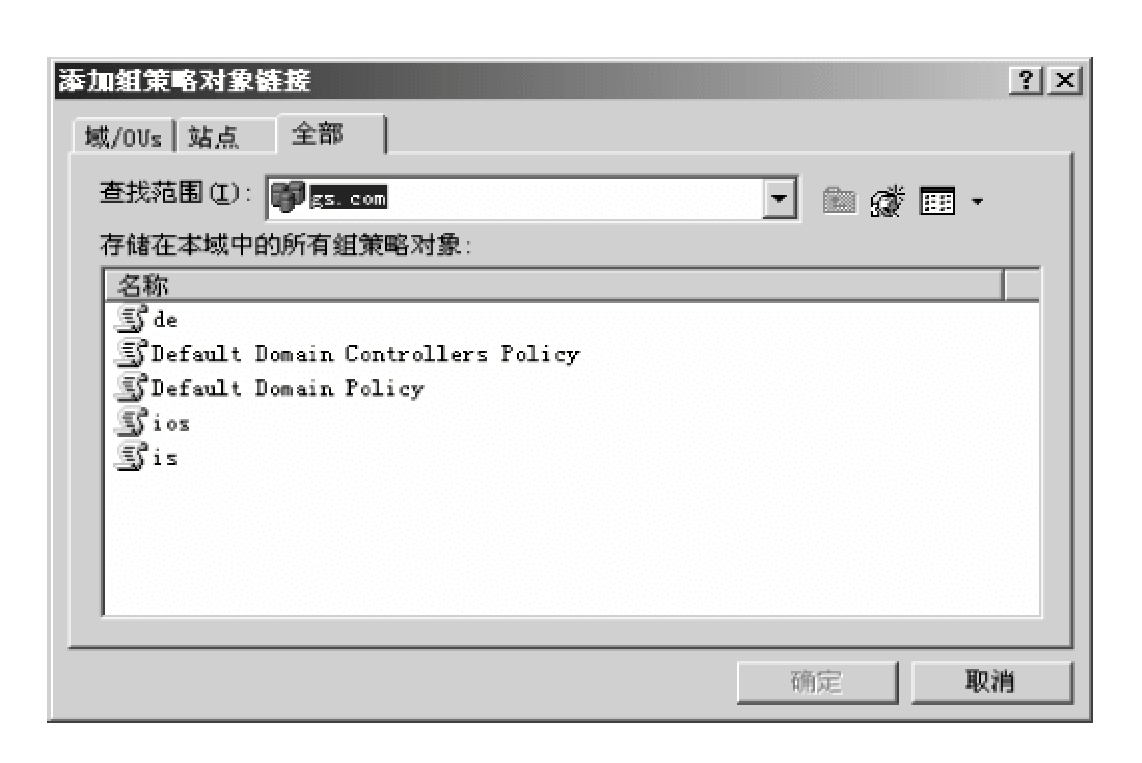


图 2-72　“添加组策略对象链接”对话框“全部”选项卡



图 2-73　添加以后的组策略

到组织单位 is 上，单击“向上”、“向下”按钮可调整组策略对象的顺序，控制其对系统的配置的影响。

2.4.2　利用组策略管理用户环境实例

利用组策略按网络的规划要求进行管理，将极大地降低管理成本。管理员只需要设置一个组策略对象，然后把它施于相应的域或组织单位即可。当然管理员也可以将多个组策略对象施于一个被管理对象，取它的叠加效果。下面通过 3 个实例进行说明。

（1）隐藏用户桌面的“我的电脑”和“我的文档”图标。

（2）使某一部门的员工不能运行 Word 程序。

（3）对某部门的员工安装某一应用程序 netinfo。

注意：下列操作前提条件是已建立组织单位 abc 且内有用户 user1 并建立了组策略对象 abc。

1．隐藏组织单位 abc 的用户桌面的“网上邻居”和“我的文档”图标

（1）选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令在“Active Directory 用户和计算机”窗口的组织单位 abc 上右击，在弹出的快捷菜单中选择“属性”命令，在“abc 属性”对话框中打开“组策略”选项卡，如图 2-74 所示。

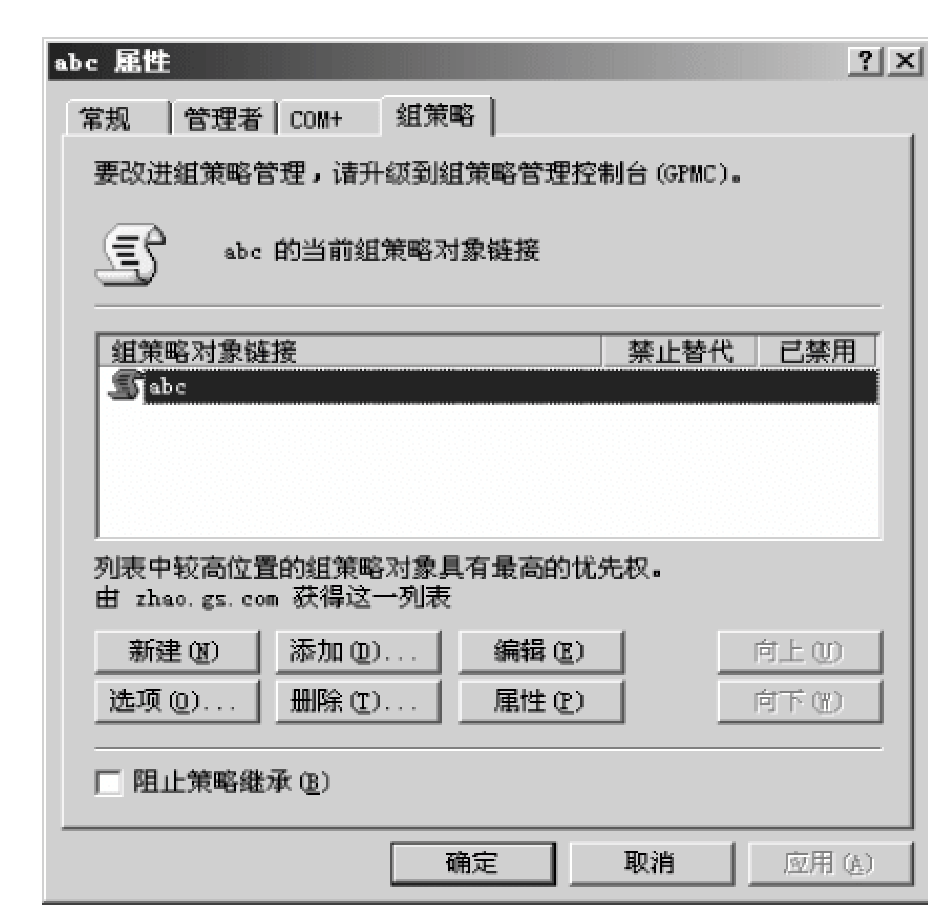


图 2-74　组织单位 abc 的属性界面

（2）单击“编辑”按钮，在“组策略编辑器”窗口选择“用户配置”→“桌面”命令，如图 2-75 所示。

（3）选择“删除桌面上的‘我的文档’图标”命令，在“删除桌面上的‘我的文档’图标属性”对



图 2-75 组策略中桌面的可选择项

话框中选择“已启用”选项，单击“确定”按钮，如图 2-76 所示。

（4）选择“删除桌面上的‘我的电脑’图标”命令，在“删除桌面上的‘我的电脑’图标属性”对话框中选择“已启用”选项，单击“确定”按钮，如图 2-77 所示。

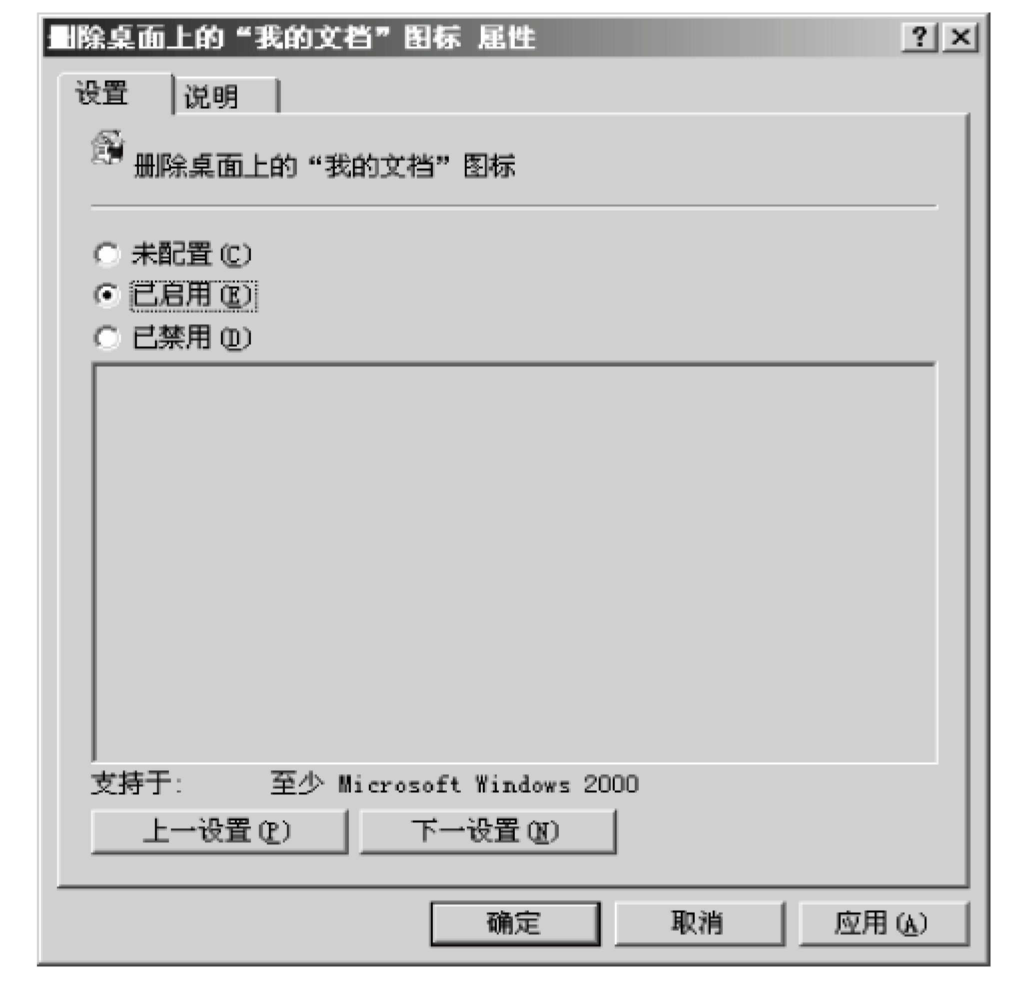




图 2-76 删除桌面上的“我的文档”图标

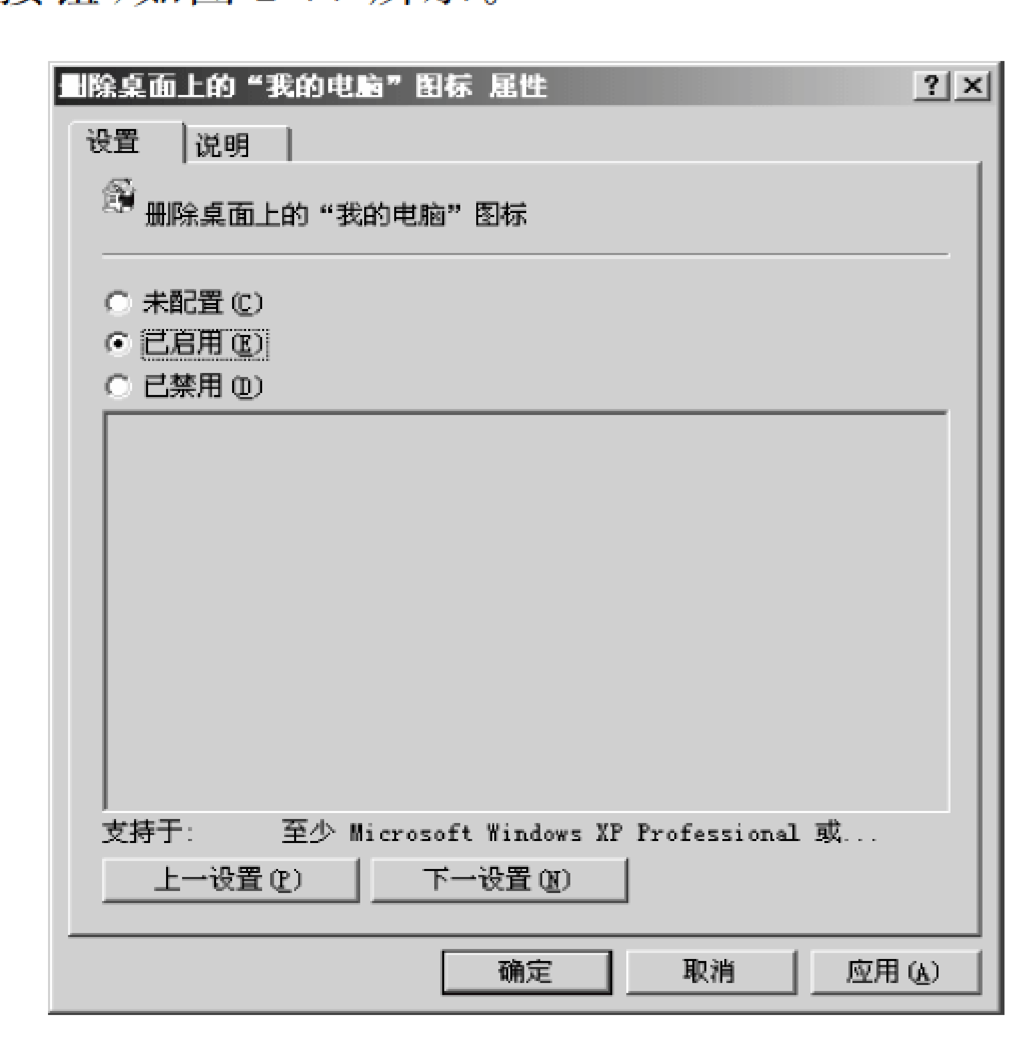


图 2-77 删除桌面上的“我的电脑”图标

（5）user1 用户桌面前后的变化如图 2-78 和图 2-79 所示。



图 2-78　隐藏图标前的桌面



图 2-79　隐藏图标后的桌面

2．禁止组织单位 abc 的用户运行 Word

（1）打开程序“Active Directory 用户和计算机”窗口，在组织单位 abc 上右击，在弹出的快捷菜单中选择“属性”命令，在“abc 属性”对话框中打开“组策略”选项卡，如图 2-80 所示。

（2）单击“编辑”按钮，在“组策略编辑器”窗口中选择“系统”→“不要运行指定的 Windows 应用程序”命令，如图 2-81 所示。

（3）在“不要运行指定的 Windows 应用程序属性”对话框中选择“已启用”单选按钮，如图 2-82 所示。

（4）单击“显示”按钮，在“添加项目”对话框中输入要被禁止的程序 winword.exe，如图 2-83 所示。

（5）单击“确定”按钮，使组策略生效。用户运行 Word 时将出现如图 2-84 所示的“限制”提示框。

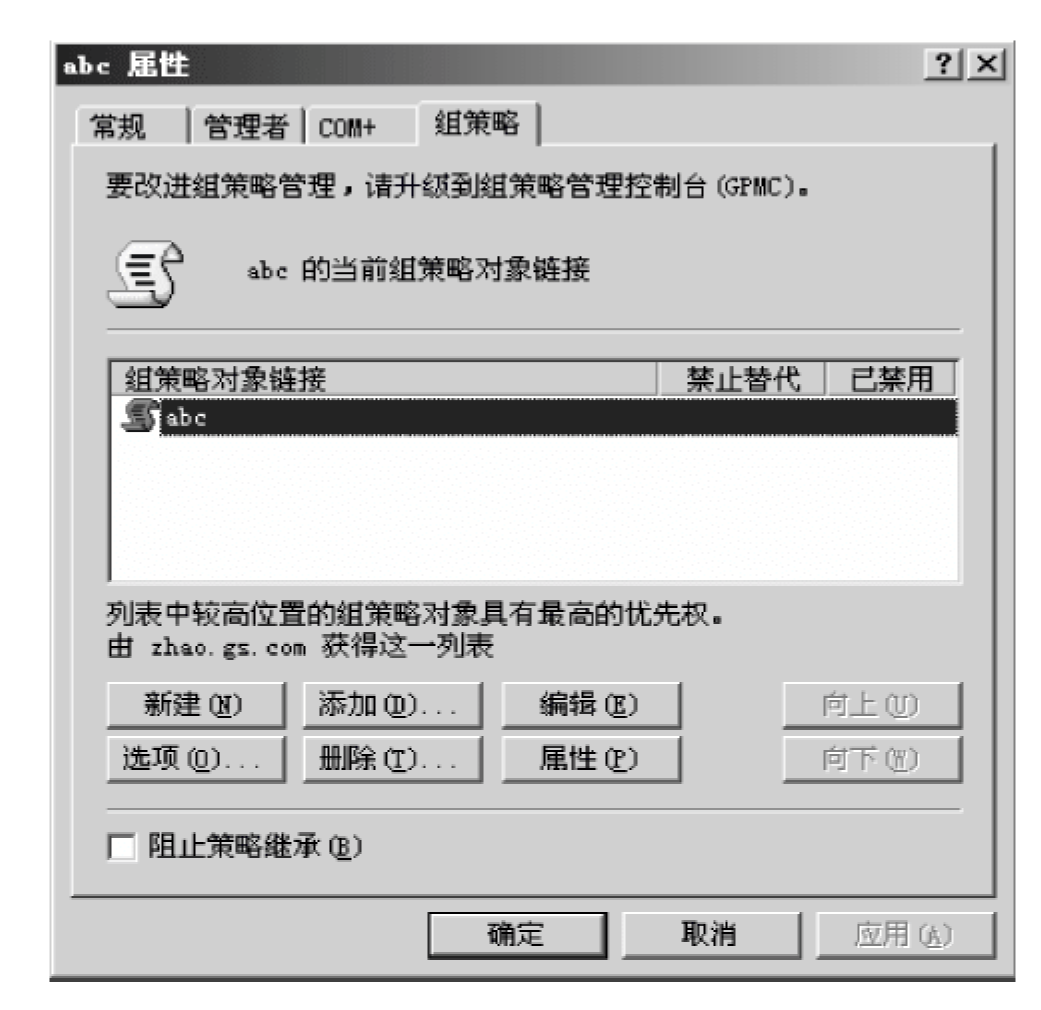
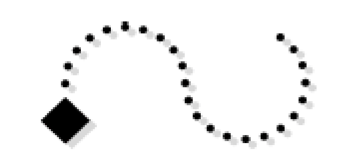


图 2-80　“abc 属性”对话框

3．为组织单位 abc 用户安装应用程序 NetInfo

使用组策略部署应用程序有发布和指派两种。发布需要用控制面板中的添加删除程序来协助安装。指派则是自动安装程序的快捷方式，等用户应用时再进行安装。被安装程序的格式必须是.msi，msi 是网络安装版的缩写。应用程序.NetInfo.msi 已经放在服务器上的共享文件夹 abc 内。



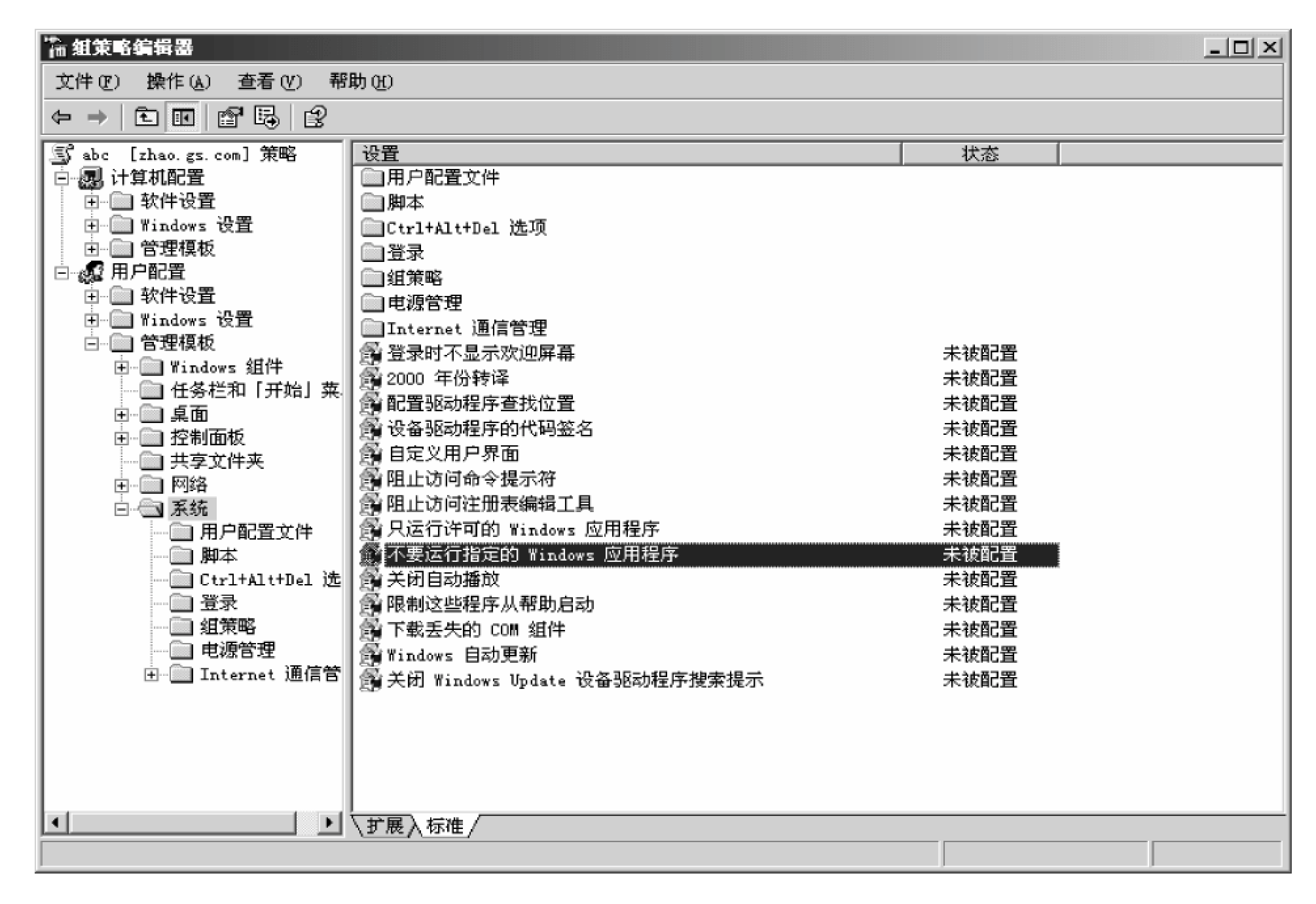


图 2-81　组策略中系统的设置

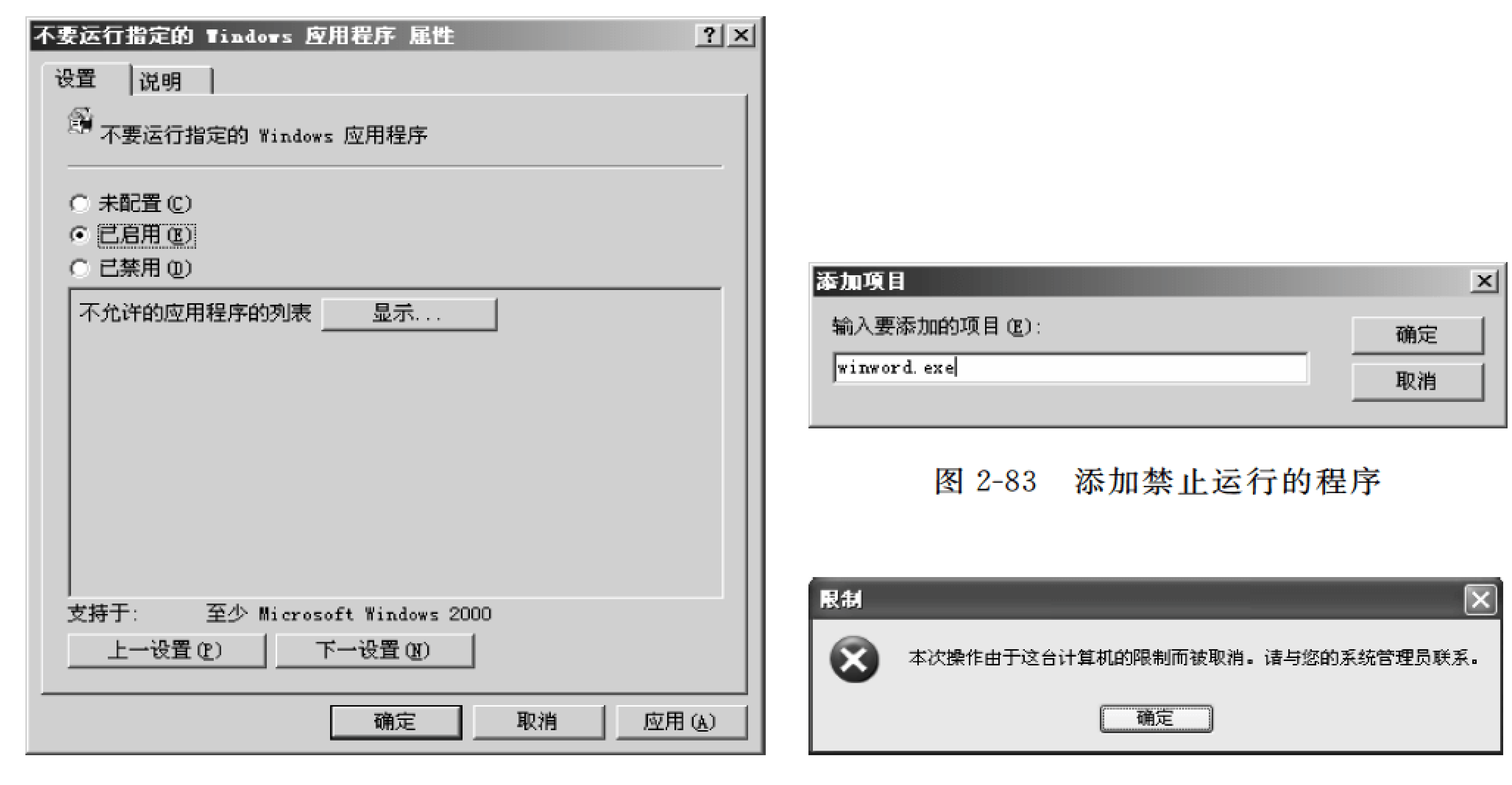


图 2-83　添加禁止运行的程序

图 2-82　属性设置界面

图 2-84　用户运行 Word 时得到的提示

(1) 打开“Active Directory 用户和计算机”窗口,在“组织单位 abc”上右击,在弹出的快捷菜单中选择“属性”命令,在“abc 属性”对话框中打开“组策略”选项卡,如图 2-85 所示。





图 2-85　组织单位 abc 的属性

（2）单击“编辑”按钮，在“组策略编辑器”窗口选择“用户配置”→“软件设置”命令，如图 2-86 所示。

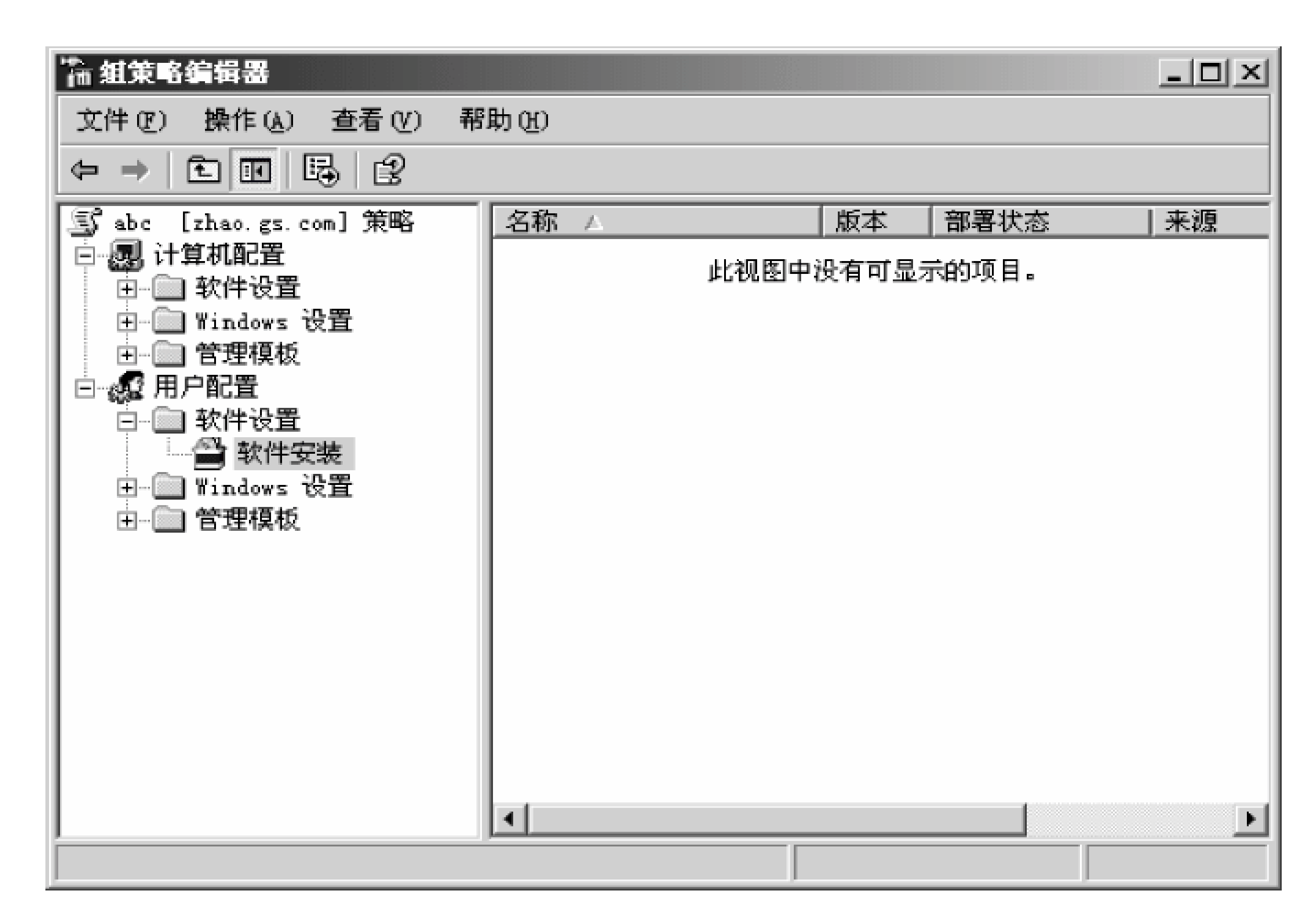


图 2-86　组策略界面

（3）右击“软件安装”，在弹出的快捷菜单中选择“新建”→“程序包”命令，如图 2-87 所示。

（4）在“打开”对话框的“查找范围”下拉列表框中选择共享文件夹 abc，并选中要安装的程序，如图 2-88 所示。

（5）单击“打开”按钮，在“部署软件”对话框中选择“已指派”单选按钮，如图 2-89 所示。

（6）单击“确定”按钮，NetInfo 程序就安装完毕，如图 2-90 所示。



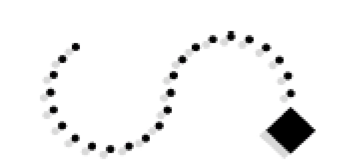
图 2-87 新建程序包



图 2-88 选择要安装的程序



图 2-89 “部署软件”对话框



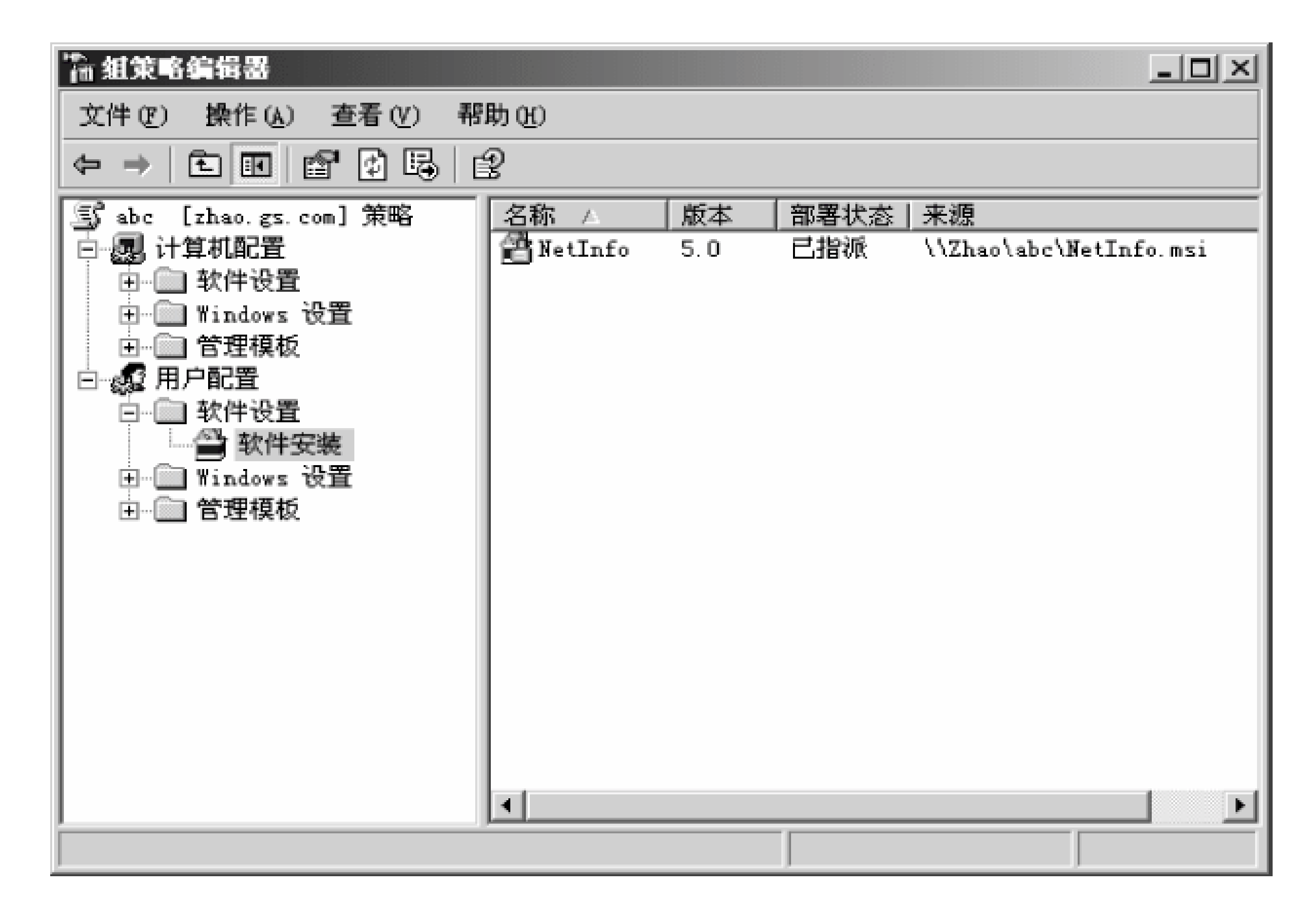


图 2-90　设置完成

使组策略生效，以 user1 用户登录，即可在"开始"菜单中见到 NetInfo 的图标。

2.5　综合实训

实训目的：学习用活动目录管理局域网，并学会用组策略控制用户和计算机的设置。

实训案例：某单位局域网需进行如下设置：

- 前台组的计算机只能运行 Office 和 IE。
- 财务组用户的"开始"菜单中不能有"运行"项目。

操作过程：

1. 前台组的计算机只能运行 Office 和 IE（假设前台组的计算机 JSJJYS8 已加入域）

(1) 选择"开始"→"程序"→"管理工具"→"Active Directory 用户和计算机"命令，打开"Active Directory 用户和计算机"窗口，如图 2-91 所示。

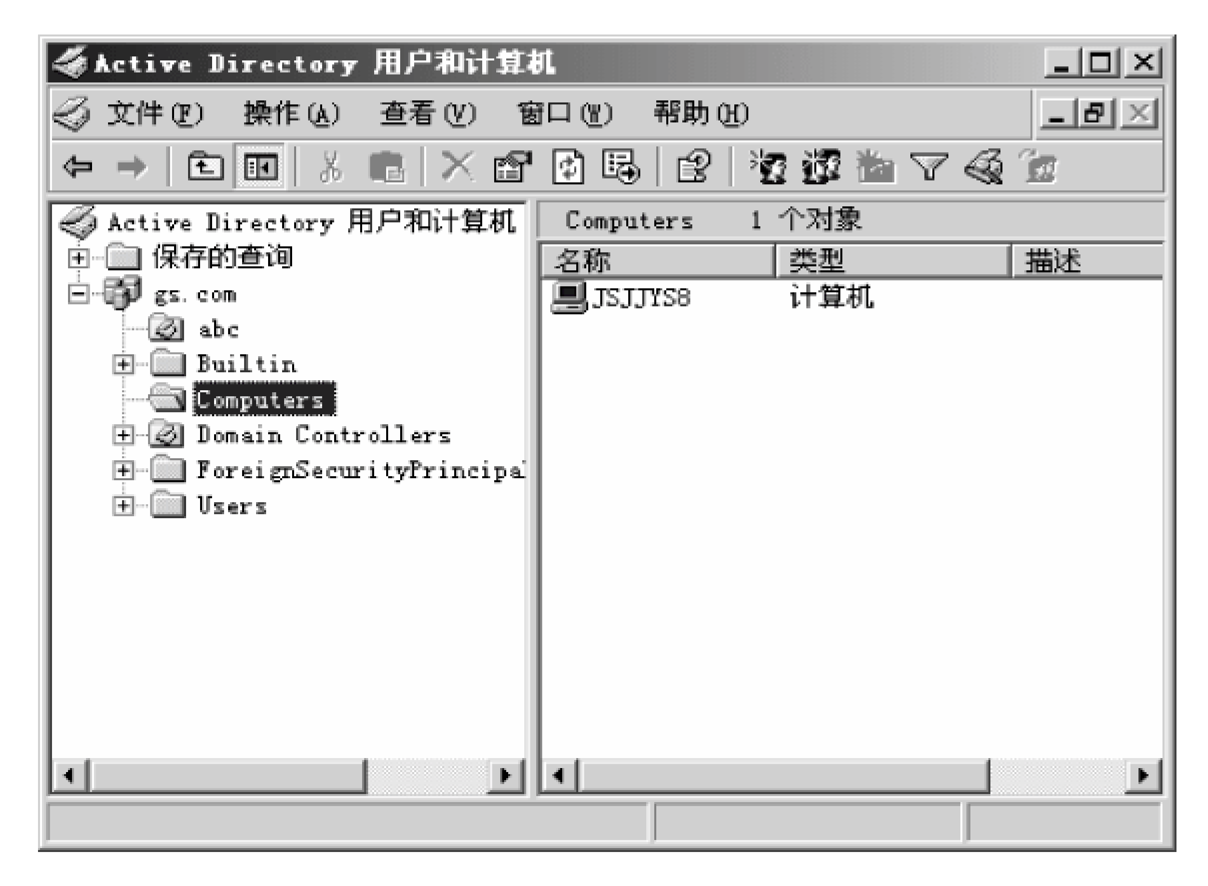


图 2-91　"Active Directory 用户和计算机"窗口

(2) 新建组织单位 qiantaizu，如图 2-92 所示。



图 2-92　新建组织单位 qiantaizu

(3) 右击 JSJJYS8，在弹出的快捷菜单中选择“移动”命令，将计算机 JSJJYS8 移入 qiantaizu，如图 2-93 所示。

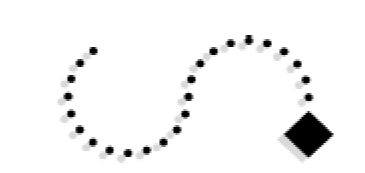


图 2-93　将计算机移入组织单位 qiantaizu

(4) 右击组织单位 qiantaizu，在弹出的快捷菜单中选择“属性”命令，在“qiantaizu 属性”对话框的“组策略”选项卡中单击“新建”按钮，建立组策略对象 qiantai，如图 2-94 所示。

(5) 单击“编辑”按钮，在“组策略编辑器”窗口选择“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”命令，如图 2-95 所示。

(6) 右击“软件限制策略”，在弹出的快捷菜单中选择“创建软件限制策略”命令，如图 2-96 所示。





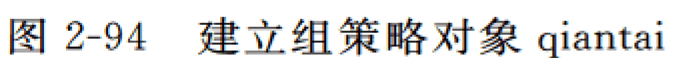

图 2-94　建立组策略对象 qiantai



图 2-95　选定软件限制策略



图 2-96　建立软件限制策略

对上述软件限制策略作如下变化：

- 安全级别设置：“不允许的”为默认的安全级别。
- 其他规则设置：新建的路径规则，如表 2-1 所示。

表 2-1　新建的路径规则

路 径 规 则	安全级别
%Windir%\System32\cmd. exe	不允许的
%Windir%	不受限的
%ProgramFiles%\Microsoft Office\Office	不受限的
%ProgramFiles%\Common Files\Microsoft Shared\	不受限的
%ProgramFiles%\Common Files\System	不受限的
%ProgramFiles%\Internet Explorer\	不受限的
\\logonsrv\logonscripts $	不受限的
C:\Documents and Settings	不受限的

• 当默认安全级别设定为不允许时，系统为了保证不会锁定用户自己或其他用户的常规操作，自动生成了 4 条路径规则，如表 2-2 所示。

表 2-2　默认安全级别为“不允许的”路径设置

路 径 规 则	安全级别
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	不受限的
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe	不受限的
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32*.exe	不受限的
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	不受限的

将其中的第 4 条路径改为%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\ Microsoft Office。

操作分析：本操作中的应用程序安装是按默认路径进行的。上述条目中以%开头和结尾的是环境变量或系统变量，表示应用程序的安装路径。有些条目使用了本实验机的绝对路径，可针对实际情况进行调整。整个操作的核心是使有些应用程序所在的文件夹有运行权，使另外一些应用程序不具有运行权。

2. 财务组用户的“开始”菜单中不能有“运行”项目

操作步骤(1)～(4)与上例的(1)～(4)相同，只是将组织单位 qiantaizu 换成组织单位 caiwuzu，将计算机 JSJJYS8 移入组织单位换成将用户 user1 移入组织单位 caiwuzu，将组策略对象 qiantai 换成组策略对象 caiwu。

(5) 单击“编辑”按钮，在“组策略编辑器”窗口选择“用户配置”→“管理模板”→“任务栏和「开始」菜单”→“从「开始」菜单中删除‘运行’菜单”命令，如图 2-97 所示。

(6) 在“从「开始」菜单中删除‘运行’菜单属性”对话框中选中“已启用”单选按钮，单击“确定”按钮，如图 2-98 所示。

(7) 使组策略生效，以 user1 登录 caiwuzu 计算机，即可看到“运行”菜单已删除，如图 2-99 所示。

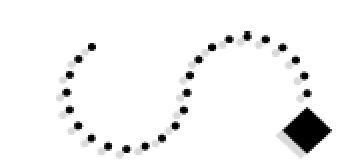




图 2-97　在组策略中删除"运行"菜单



图 2-98　设置删除项目启用



图 2-99　实际效果

2.6　本章小结

本章在单域模式下介绍了 Windows Server 2003 活动目录的使用，重点说明了域、用户、组、组织单位的概念，管理操作及使用方法，同时介绍了组策略概念、组策略的内容以及组策略的编辑方法，通过实例介绍了如何用组策略在基于组织单位的基础上对用户或计算机进行管理的方法。希望读者将 Windows 2003 操作系统提供的基于局域网

的服务器/客户机管理方法与对等网的管理方法进行比对，举一反三，在今后的管理中熟练使用。

2.7 本章习题

1. 简述域、组、组织单位的区别。
2. 简述本地用户、域用户的区别。
3. 禁止某单位行政组计算机运行 Outlook Express。
4. 只允许某单位服务组用户运行 Microsoft Office。
5. 简述组策略的执行次序。

第 3 章

Windows 2003 服务器的架设

本章内容：

前两章主要学习了 Windows 2003 对于网络资源的管理功能。本章主要介绍 Windows Server 2003 网络服务功能，即对 Internet/Intranet 环境的支持，这里只介绍 DNS、DHCP 及 IIS 的服务功能。希望通过学习为网络系统集成和网络应用的开发打下一定的基础。

本章重点：

① 了解 DNS、DHCP 的工作原理，掌握 DNS 和 DHCP 的配置方法与技巧，学会加强其安全性的管理手段。

② 理解 IIS 的作用，掌握用 IIS 架设 WWW、FTP 站点的方法，掌握管理站点的方法与技巧，理解使用虚拟目录的意义。

③ 通过学习掌握架设服务器的一般方法，并能用第三方提供的软件架设 Internet/Intranet 环境下常用的服务器。

传统局域网的资源共享方式已不能满足人们对信息的需求，人们迫切地需要更多形式的网络服务。Windows 2003 操作系统顺应这一变化，推出了基于 TCP/IP 协议的各种组件来支持常见的网络服务，下面就进行简单的介绍。

3.1 DNS 服务器的架设

3.1.1 DNS 原理

DNS(Domain Name System，域名系统)是 TCP/IP 网络架构中非常重要的一个系统。域名系统 DNS 的出现，满足了庞大网络的域名翻译需求。DNS 可以将主机名转换成实际的 IP 地址，还可以把 IP 地址翻译成主机名，这种翻译的过程称为域名解析。负责域名解析的服务器称为域名服务器。

DNS 服务器用人们熟悉的英文名称(例如，www. baidu. com)代替其对应的 IP 地址(例如，202. 108. 22. 5)来完成相应的地址定位和服务。

在因特网中各网络的域名服务器构成了分布的域名数据库系统，每一个网络的域名系统维护自己所在域的数据库信息，各 DNS 按照一定的协议提供数据库信息检索和查询。为了保证 DNS 服务能够提供可靠的解析服务，通常在一个网络内要建立一个主 DNS 服务器和至少一个辅 DNS 服务器。

1. DNS 域名空间

DNS 的结构是一种树型结构，此结构组成的形式称为域名空间，如图 3-1 所示。

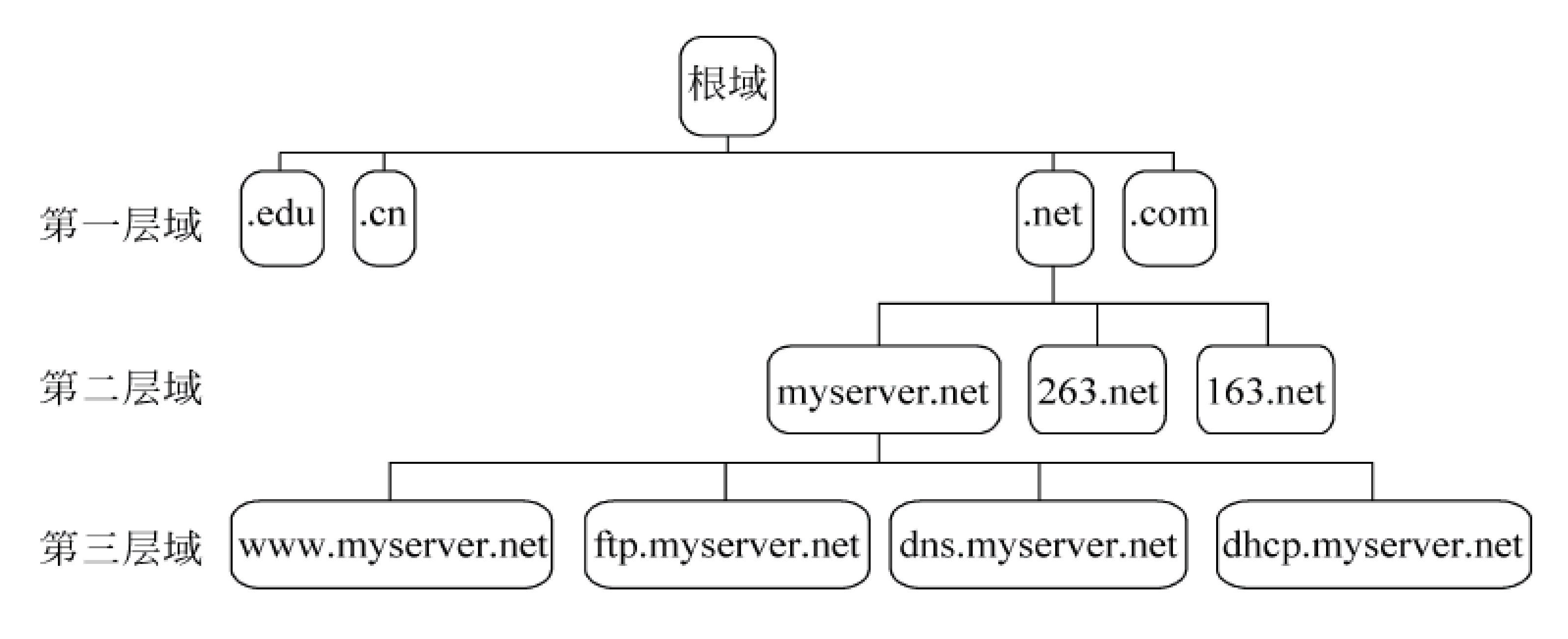


图 3-1　域名系统树型结构

域名结构由若干部分组成，各分量之间用点号隔开，其格式如下：

……. 三级域名. 二级域名. 顶级域名

(1) 根域(Root Domain)。根域是树的顶级域。在域名应用时，根域的尾部用“. ”表示。利用根域，DNS 域名才能被认为是一个完整名称并指向 DNS 域名称树中的确切位置，这样的域名形式称为全限定域名(FQDN)。如 myserver. net. 在末尾使用了点号“. ”。

(2) 顶级域。现在常用的最高层顶级域名 TLD(Top Level Domain)有 3 大类。

- 国家顶级域名 nTLD 采用 ISO 3166 的规定，例如，cn 表示中国，us 表示美国等。
- 国际顶级域名 iTLD 采用 int，一般保留供国际组织使用。
- 通用顶级域名 gTLD，例如，com(用于商业组织)、net(用于提供网络和通信服务的组织)、edu(用于教育机构)、org(用于商业非赢利组织)、gov(用于政府机构)、mil(美国军事机构)等。

2. DNS 的区域构成

DNS 区域是域名空间结构中的一部分，每一个 DNS 服务器都会有一个区域，它存储了这个区域中主机的数据，用来存储这些数据的文件就称为区域文件。一个区域所包含的范围必须是一个连续的空间区域，每个区域拥有各自的 DNS 数据库文件来记录该区域的数据。

DNS 区域有标准主区域、标准辅助区域和 Active Directory 集成区域 3 种类型。

(1) 标准主区域存储着主机名和 IP 地址的解析记录。

(2) 标准辅助区域主要存储主区域的只读副本，当主区域服务器工作负载过重时，辅助区域将分担一部分工作，达到负载平衡的目的。

(3) Active Directory 集成区域存储本域的主机名和 IP 地址的解析记录。只有当此

DNS 所在服务器位于域控制器时方有效。

3. DNS 的查询方式

DNS 的主要目的是能够将用户提交的域名或 IP 地址转换为其相对应的 IP 地址和域名，这一过程称为名称解析。DNS 为了能够完成此操作，则需查找一个数据的集合，对于这样的数据进行查找，其方法通常有两种。

（1）递归。若域名为 abc. myserver. net 的主机想要知道另一个域名为 www. r. abc. net 的主机的 IP 地址，可以先向其本地域名服务器 dns. myserver. net 提出查询请求。由于本域 DNS 不知道其他域的信息，查不出此域名对应的 IP 地址。继而向其上一级 net 域的 DNS 服务器 dns. net. 提出查询。根据被查询的域名中的 abc. net，再向授权域名服务器 dns. abc. net 发送查询报文，然后将此查询交给 dns. r. abc. net。此域名服务器记录了 www. r. abc. com 的 IP 地址，则将此查询结果按照原来的提交路径反向传送回给 abc. myserver. net 主机。这种方法称之为递归查询。

（2）递归与迭代相结合。在递归查询中，各服务器都要参与查询。为了减轻顶级域的域名服务器的工作负担，根域名服务器收到本域中的查找本域中其他子域的申请时，可以直接将申请发送给其域名服务器，查询结果也由此服务器直接提交给提出请求的域名服务器。

3.1.2 DNS 的服务器安装

DNS 的服务器的安装步骤：

（1）选择“开始”→“控制面板”→“添加或删除程序”命令，在弹出的“添加或删除程序”窗口中选择“添加/删除 Windows 组件”命令，弹出如图 3-2 所示的“Windows 组件向导”对话框。

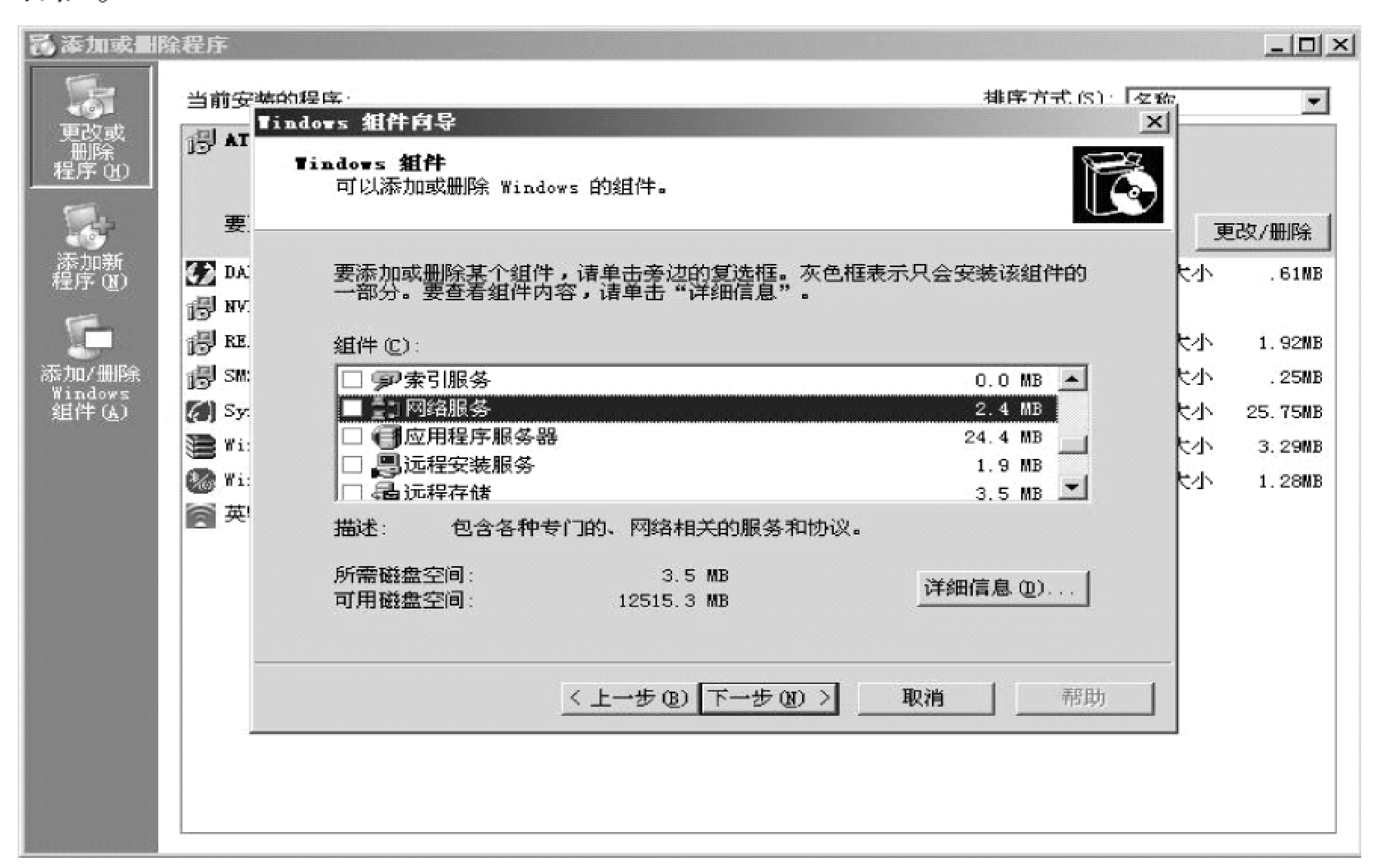


图 3-2 安装 DNS 服务

（2）选择“网络服务”复选框，并单击“详细信息”按钮，弹出如图 3-3 所示的“网络服务”对话框。

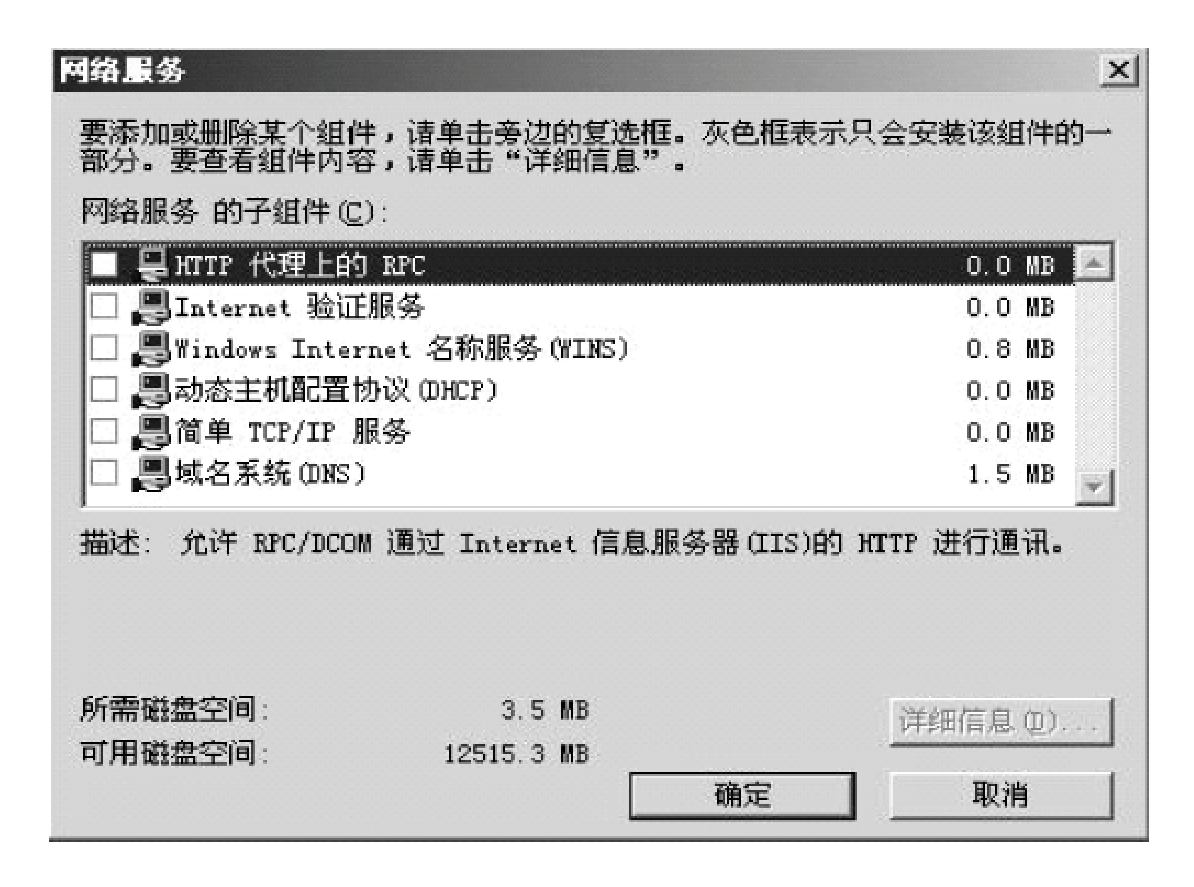


图 3-3 选择需要安装的组件

（3）选择“域名系统(DNS)”复选框，并单击“确定”按钮，在图 3-2 所示的对话框中单击“下一步”按钮，则系统会自动在服务器上安装 DNS 服务，如图 3-4 所示。

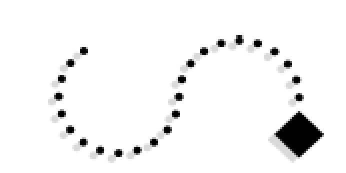


图 3-4 安装需要的服务组件

当安装完成后，单击“确定”按钮退出。至此，DNS 安装完毕。如果要使 DNS 工作，还应对其进行进一步的配置。

3.1.3 在 DNS 服务器中创建搜索区域

配置 DNS 的服务通常包括两个方面，一方面是将域名转换为 IP 地址，称为正向解析；另一方面是将 IP 地址转换为对应的域名，称为反向解析。



已知现有一个域，名称为 myserver.net，当前域服务器 IP 地址为 192.168.1.10，掩码为 255.255.255.0，对其进行配置使其成为域中的主 DNS 服务器。

1. 建立 DNS 服务器的正向查找区域

其操作步骤如下：

(1) 右击“正向查找区域”，在弹出的快捷菜单中选择“新建区域”命令，如图 3-5 所示。

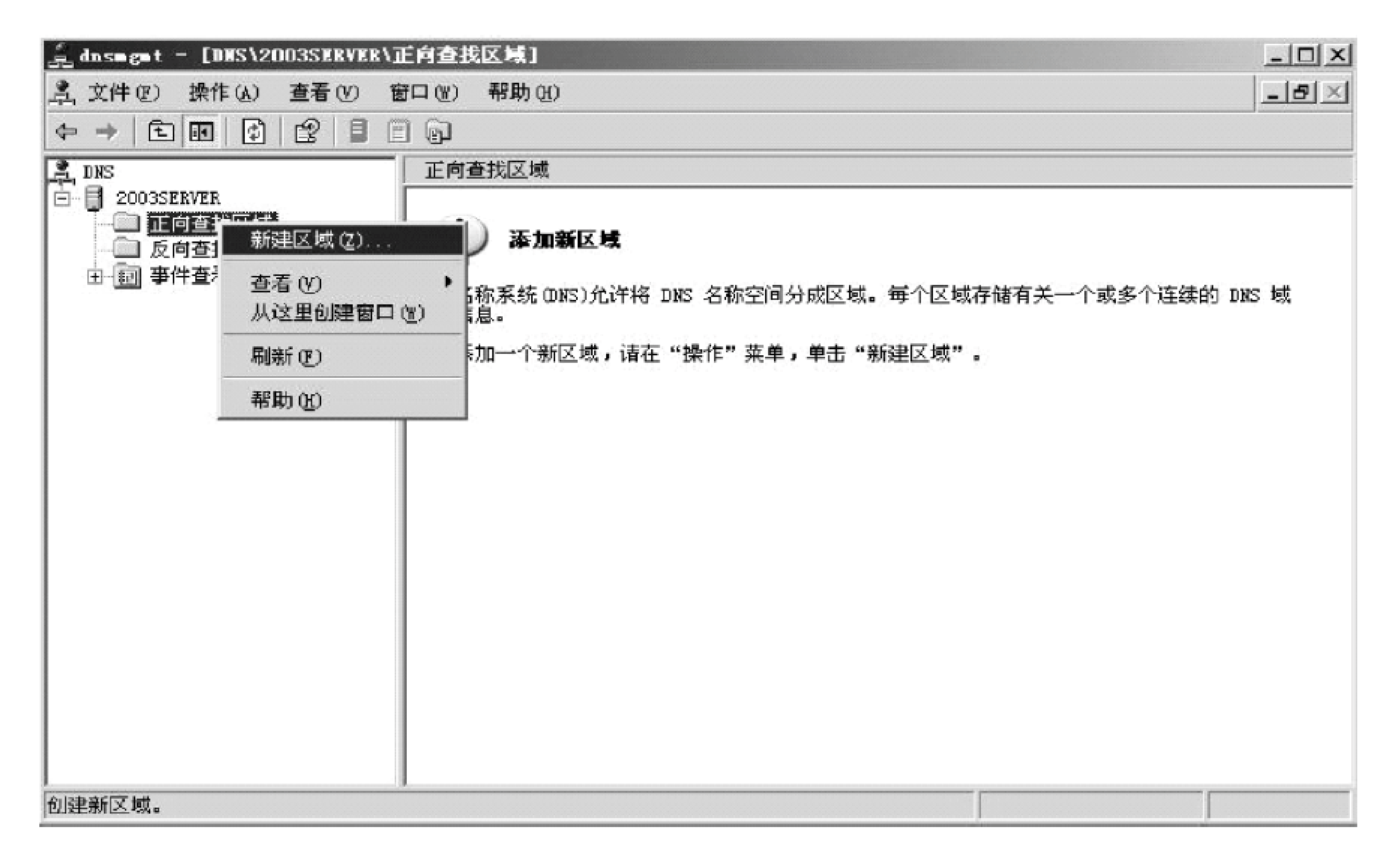


图 3-5　新建区域

(2) 在弹出的如图 3-6 所示的对话框中有 3 个单选按钮可以选择。

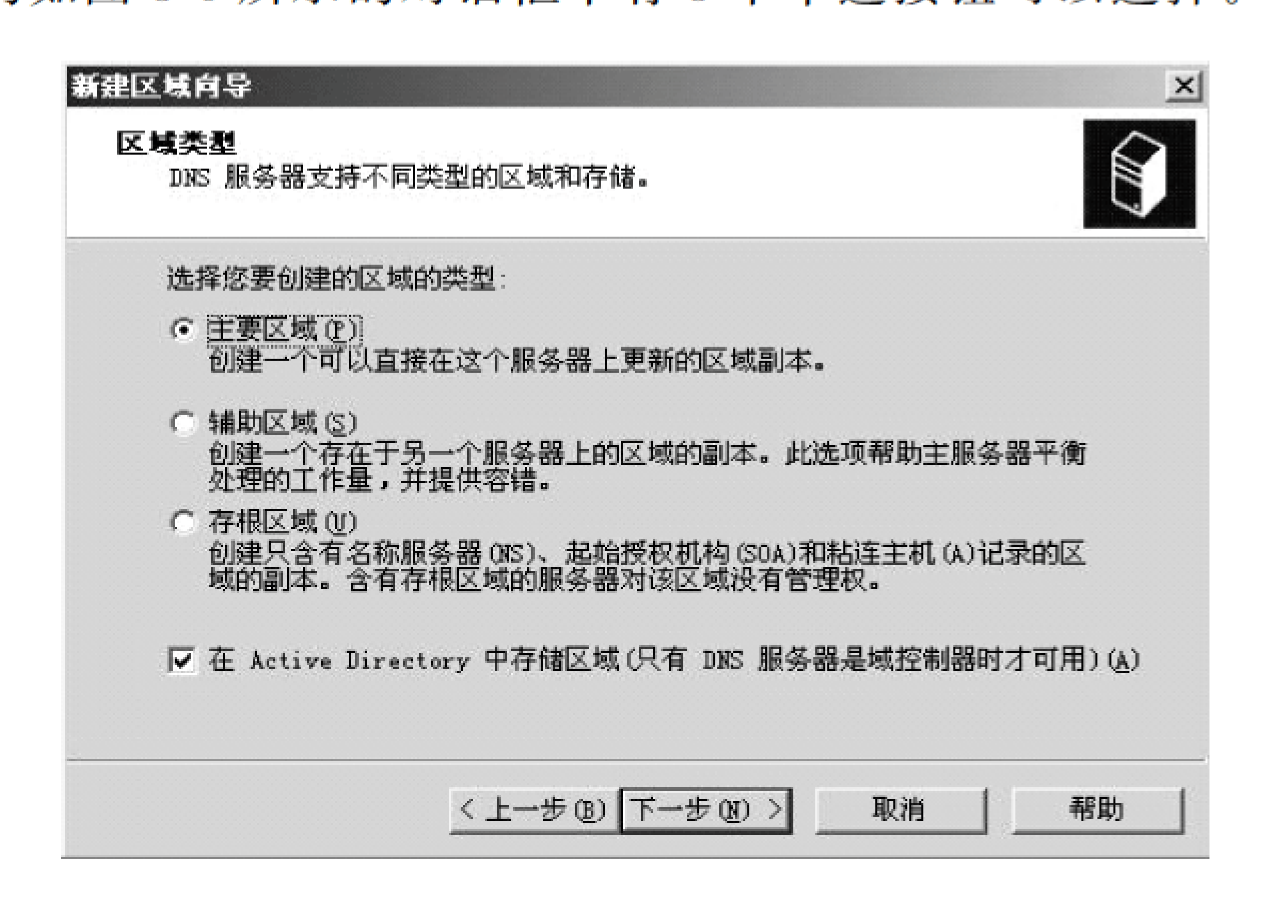


图 3-6　选择建立的正向区域类型

- “主要区域”：在本服务器上进行存储和解析的区域。
- “辅助区域”：在其他服务器上进行存储和解析的区域，只是当其服务器工作负载

过重时进行负载平衡而弃用的备用区域，也可以为主 DNS 服务器的异常进行错误处理。

- “存根区域”：用于保存根区域的信息，并不进行解析工作。

本例新建一个主 DNS 区域，所以选择“主要区域”单选按钮。

(3) 单击“下一步”按钮，弹出如图 3-7 所示的对话框，本例是对 myserver. net 域的 DNS 进行配置，所以选择“至 Active Directory 域 myserver. net 中的所有域控制器”单选按钮。

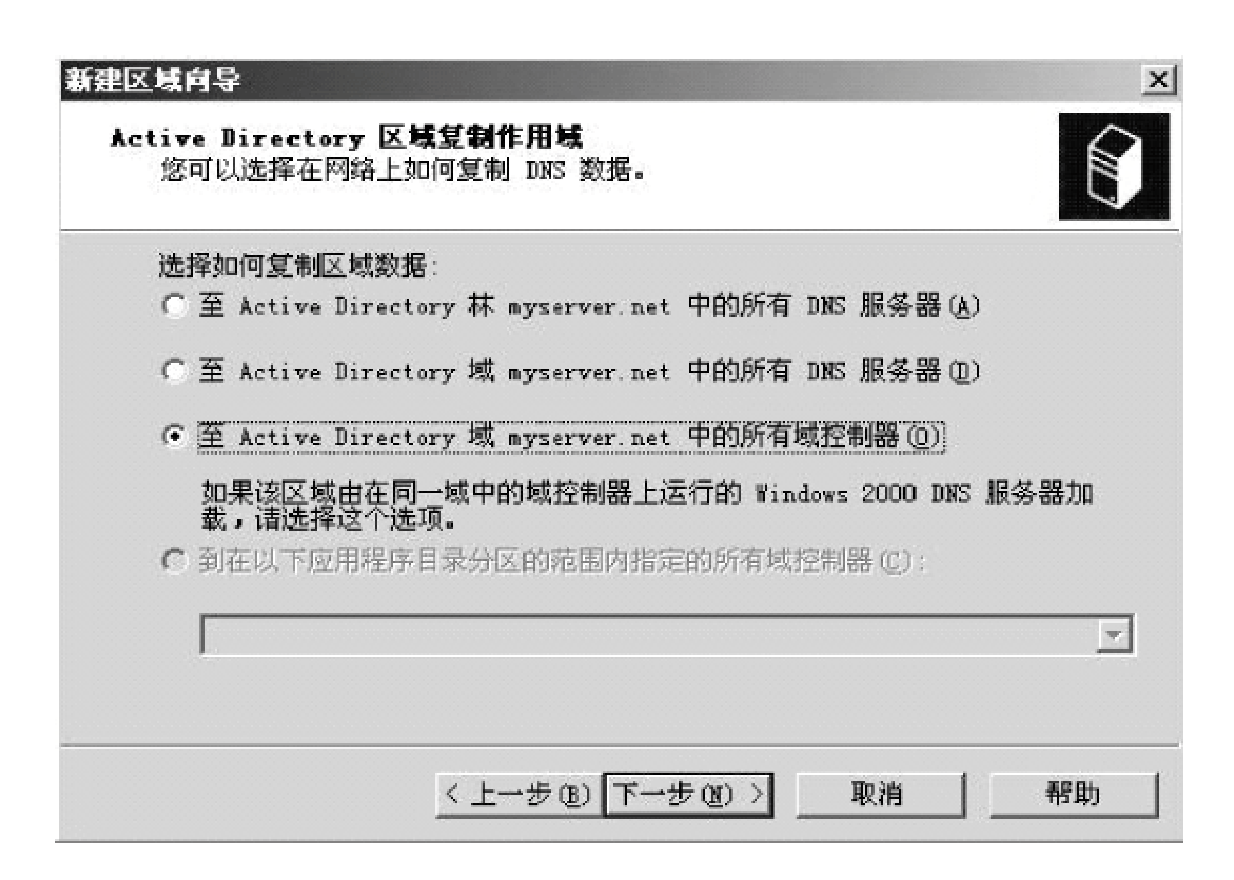


图 3-7　选择 DNS 数据复制范围

(4) 单击“下一步”按钮，弹出如图 3-8 所示的对话框。在“区域名称”文本框中输入本域的域名 myserver. net。

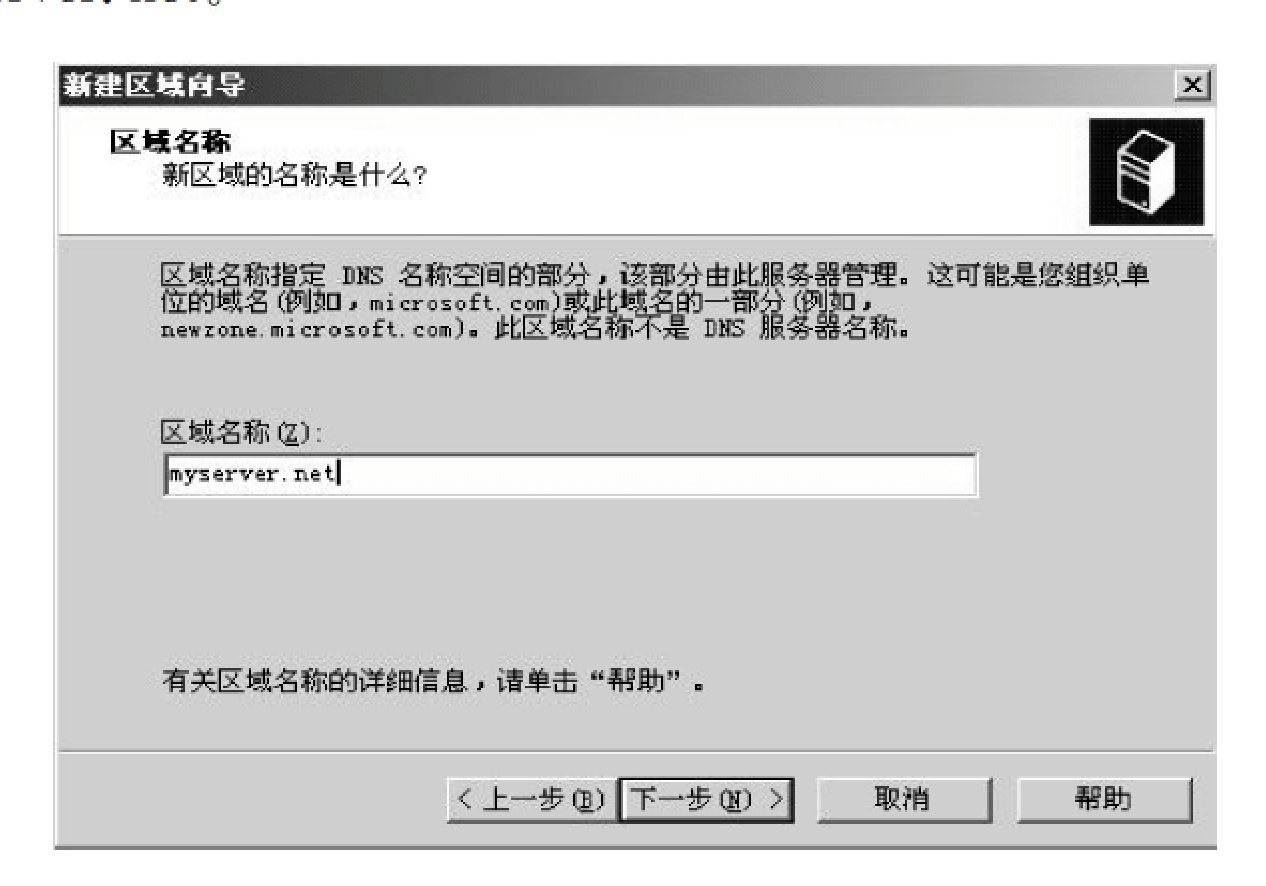
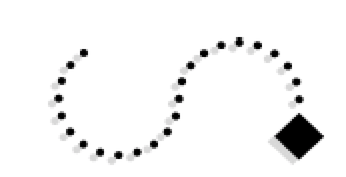


图 3-8　输入正向查找区域的名称

(5) 单击“下一步”按钮，弹出如图 3-9 所示的对话框。对新创建的 DNS 区域的动态更新进行设置，有 3 种方法：



• 只允许此域中的其他 DNS 进行动态更新。
• 允许其他非受信区域进行动态更新。
• 不允许动态更新，只能由 DNS 管理员来进行手动更新。

本例选择“只允许安全的动态更新(适合 Active Directory 使用)”单选按钮。

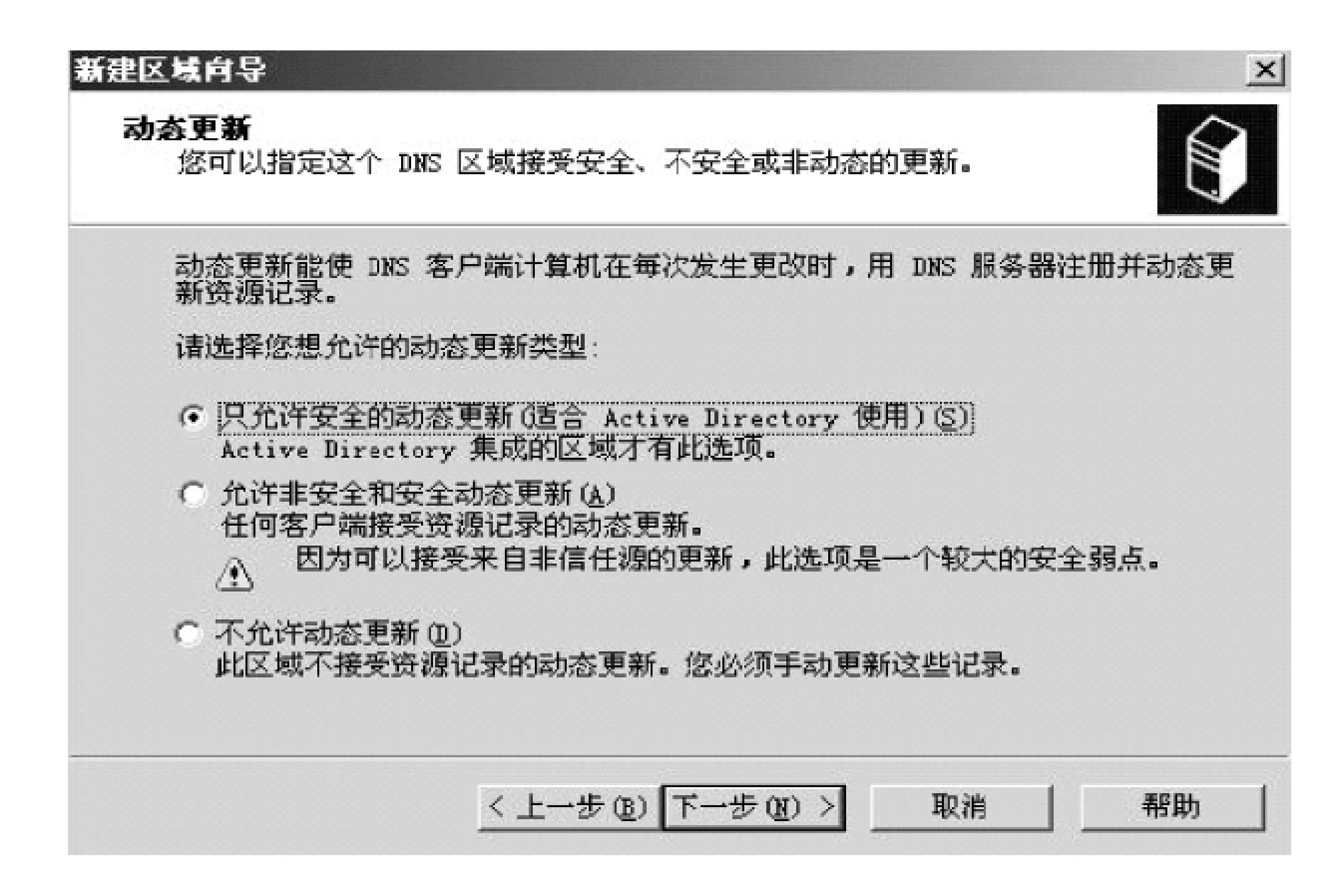


图 3-9　DNS 区域更新类型的设置

(6) 单击“下一步”按钮，弹出如图 3-10 所示的对话框。单击“完成”按钮，完成正向区域设置。

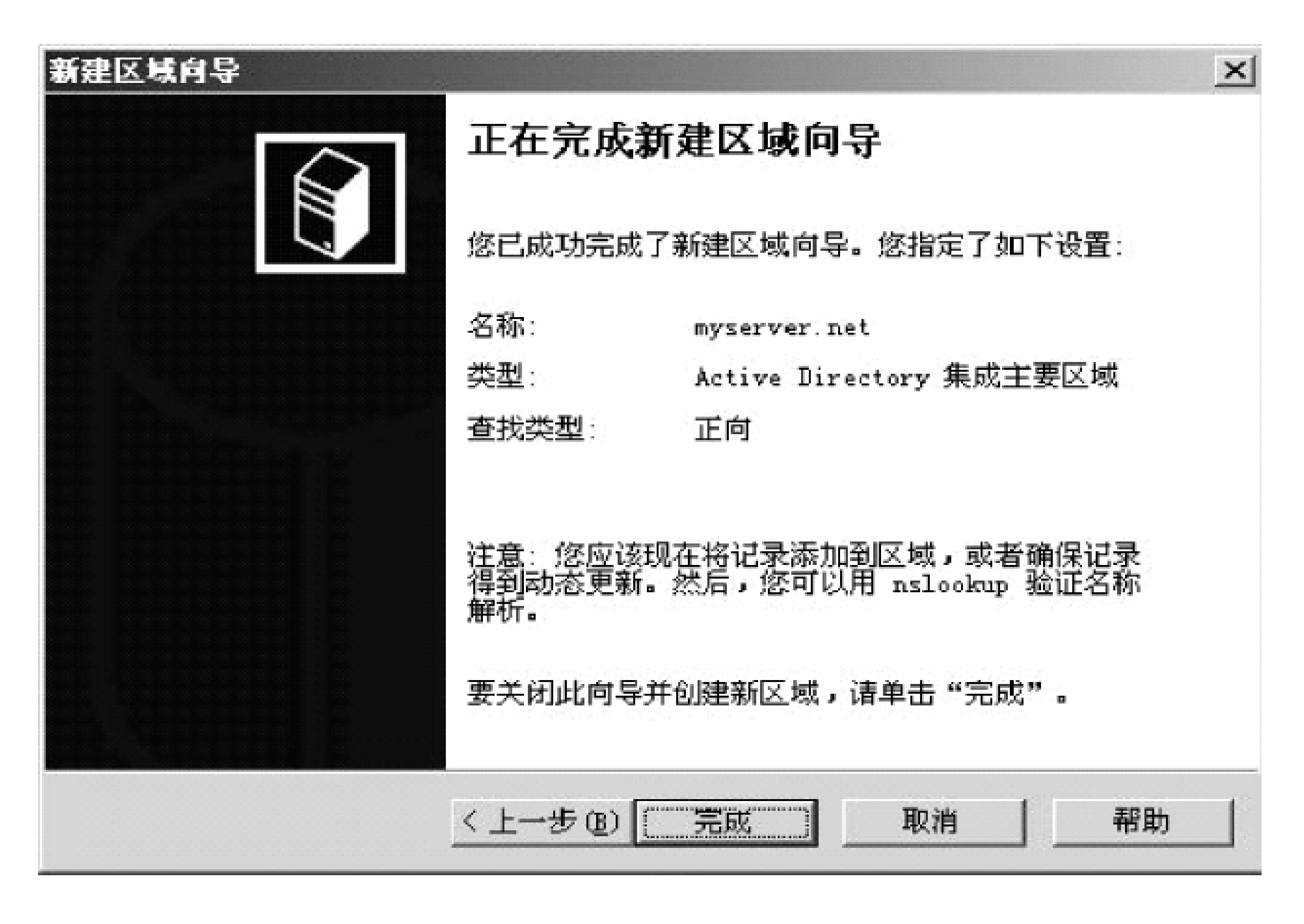


图 3-10　完成正向区域设置

2. 建立 DNS 服务器的反向查找区域

其操作步骤如下：

(1) 如图 3-11 所示，右击“反向查找区域”，在弹出的快捷菜单中选择“新建区域”命令，弹出如图 3-12 所示的对话框。

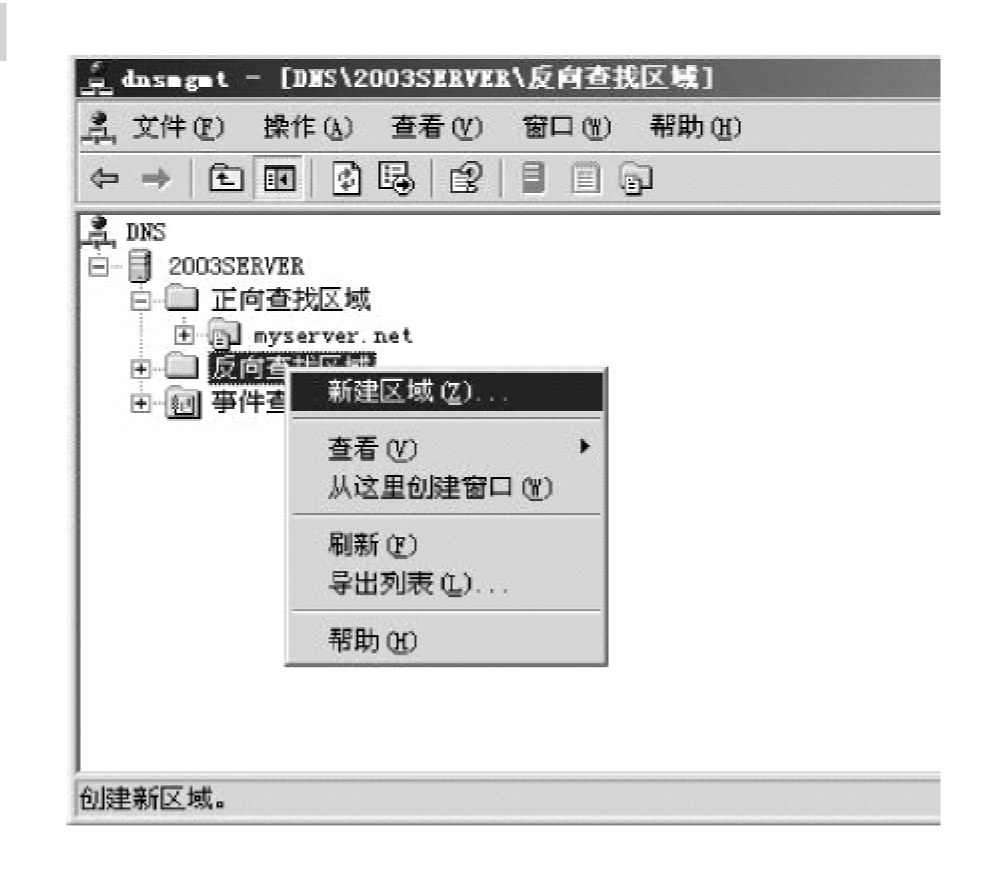


图 3-11　DNS 反向区域的建立

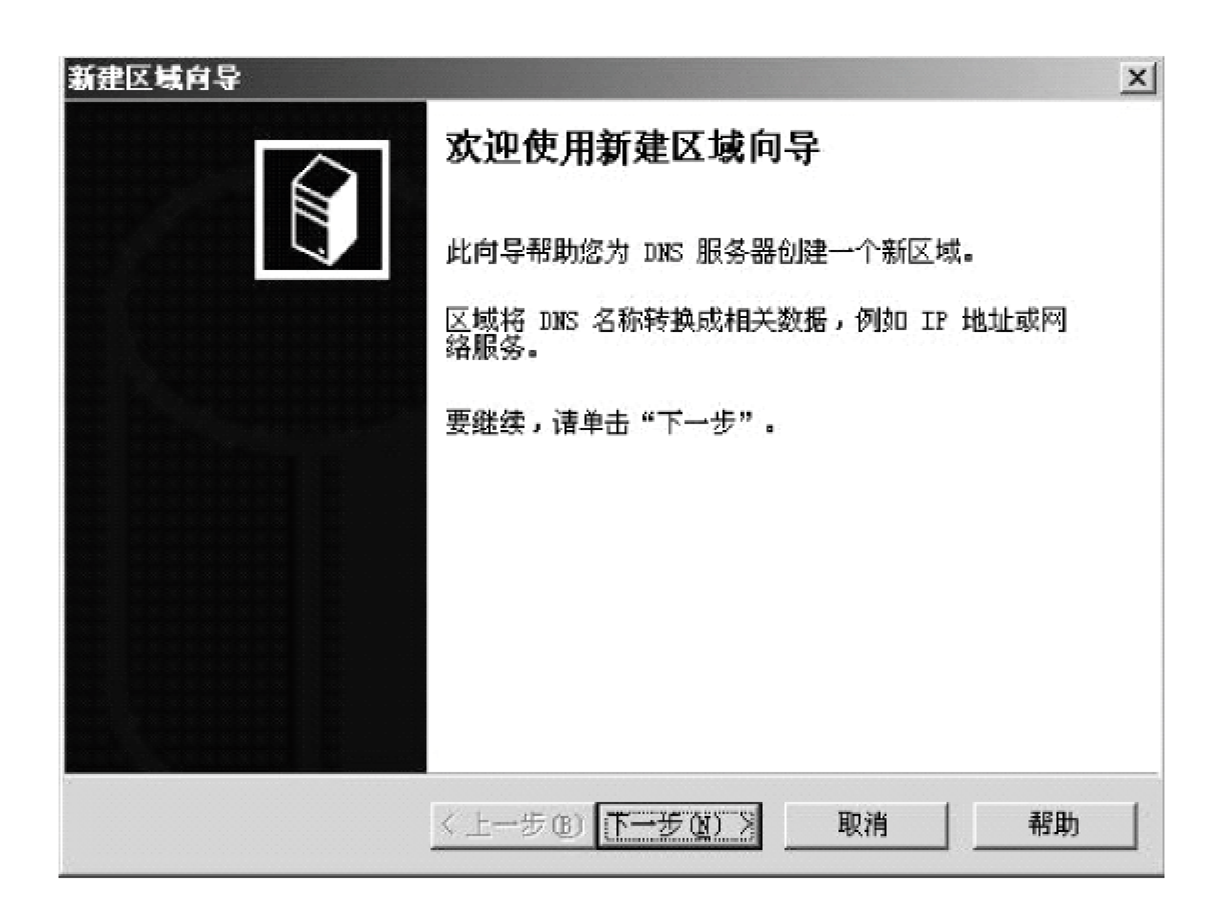


图 3-12　DNS 建立反向区域

（2）单击"下一步"按钮，弹出如图 3-13 所示的对话框，在该对话框中选择要设置的反向区域的类型。选择"主要区域"单选按钮，建立主 DNS 的反向区域。

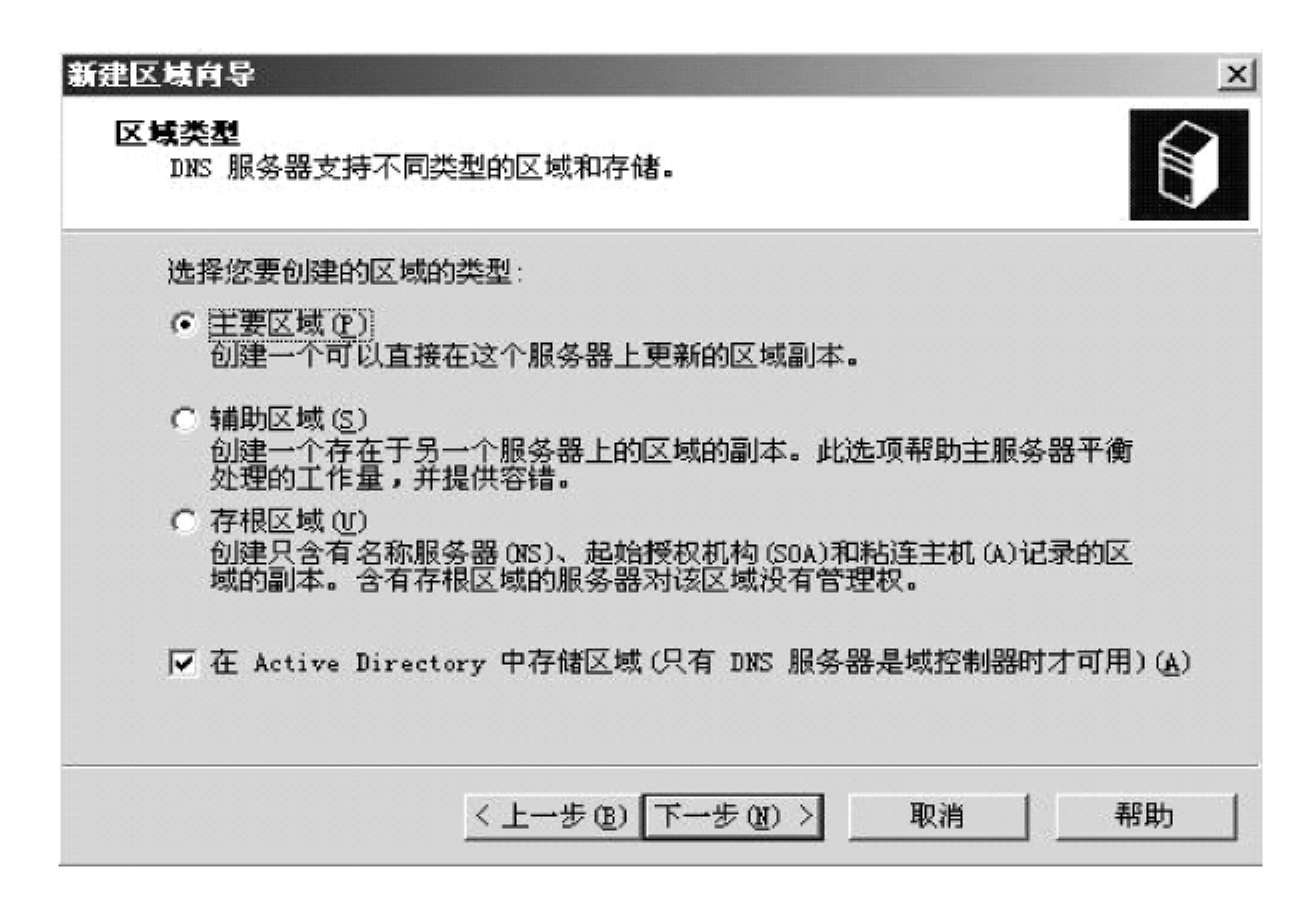


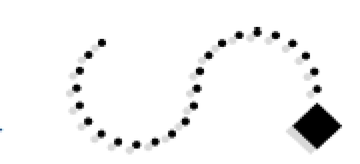
图 3-13　选择创建的反向区域类型

（3）单击"下一步"按钮，则弹出如图 3-14 所示的对话框。选择"至 Active Directory 域 myserver.net 中的所有域控制器"单选按钮。

（4）单击"下一步"按钮，弹出如图 3-15 所示的对话框。选中"网络 ID"单选按钮并在文本框中输入此 DNS 服务器解析的网段 192.168.1。在"反向查找区域名称"文本框中会自动加入其反查的区域文件的名字。

（5）单击"下一步"按钮，弹出如图 3-16 所示的对话框。在该对话框中设置 DNS 反向解析区域数据的更新类型，选择"只允许安全的动态更新(适合 Active Directory 使用)"单选按钮。

（6）单击"下一步"按钮，弹出如图 3-17 所示的对话框，单击"完成"按钮，结束反向区域的建立。



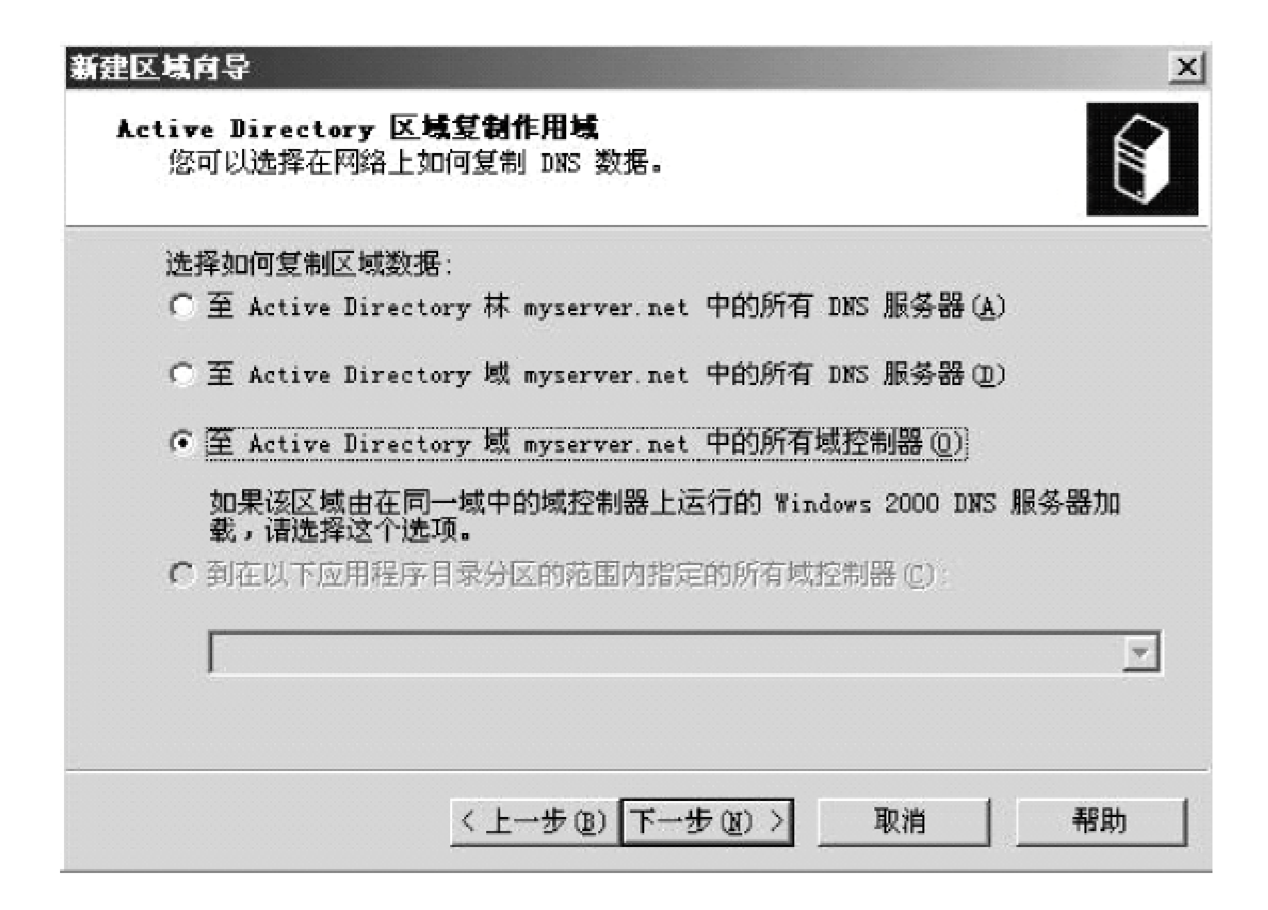


图 3-14　选择 DNS 数据复制的范围

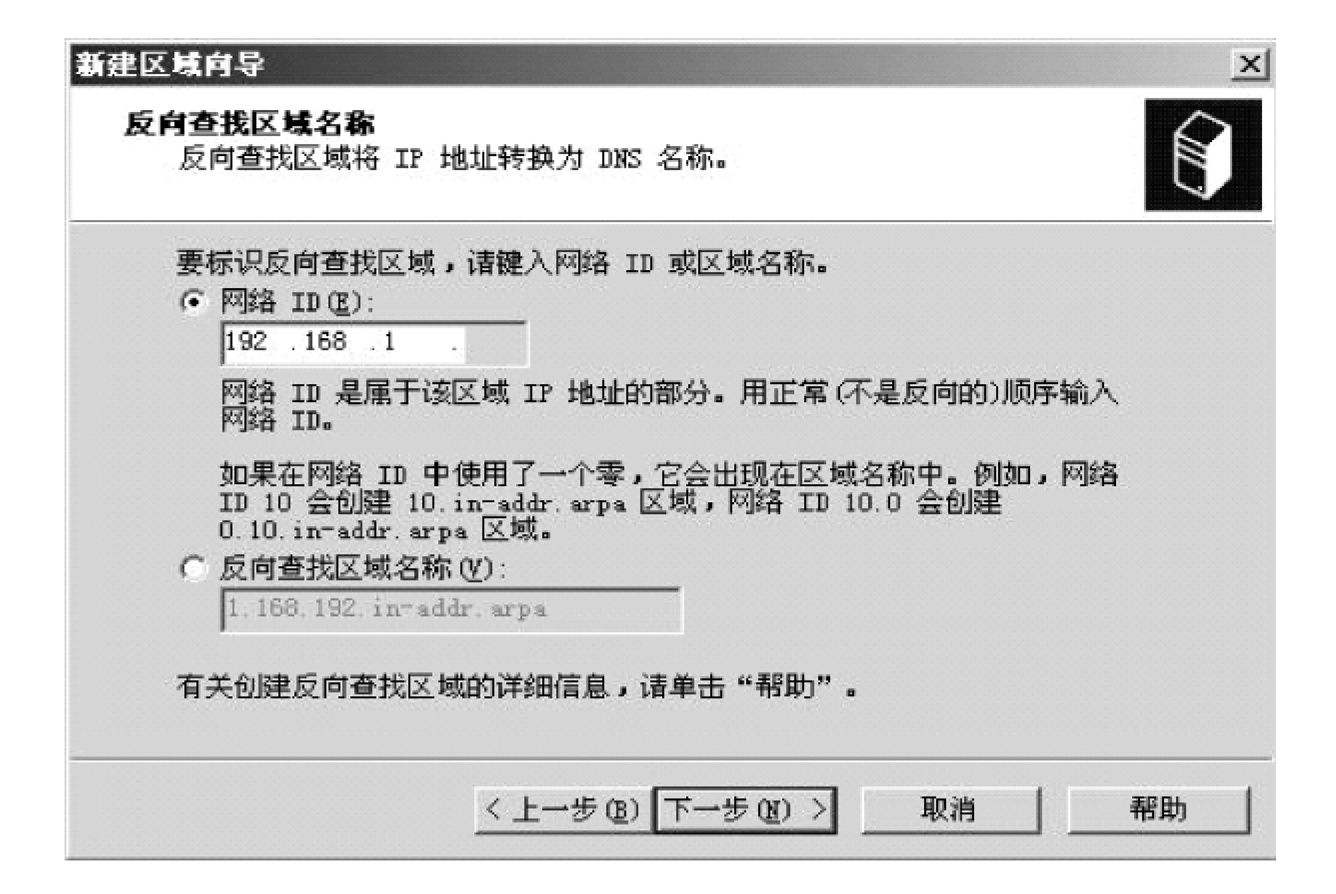


图 3-15　设置反向查找区域的 IP 地址

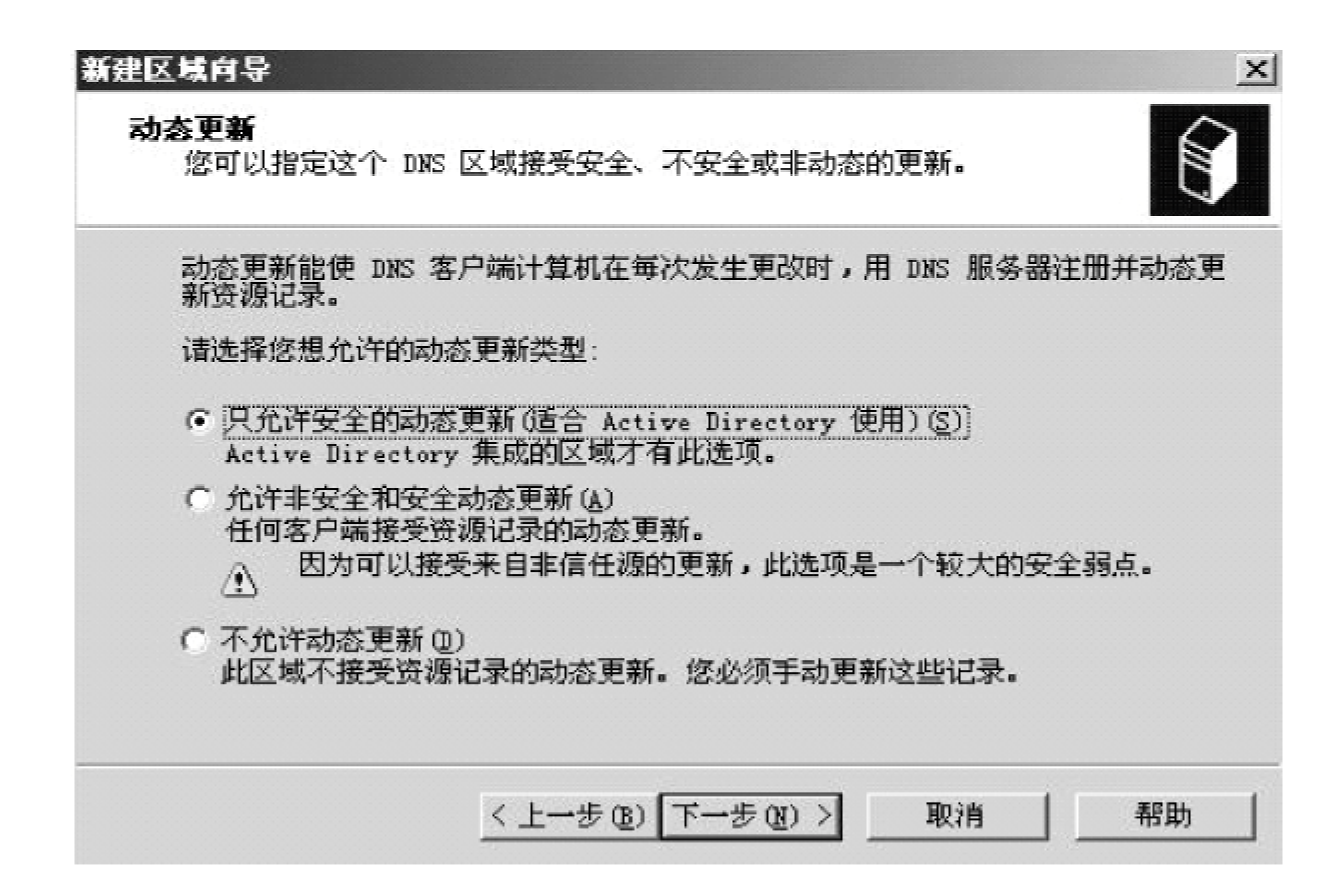


图 3-16　设置 DNS 动态更新类型



图 3-17　反向区域设置结束

3. 资源记录

新建 DNS 服务器主区域后，DNS 域管理器自动在区域中建立起始机构授权、名称服务器以及一些与域有关的主机地址信息等，这些数据称为资源记录。一般来说，资源记录包含与特定主机相关的某些信息，例如，主机名称、所有者、IP 地址或提供服务的类型。

常用的资源记录类型有：

- 起始授权机构 SOA(Start Of Authority)
- 名称服务器 NS(Name Server)
- 主机记录 A(Address)
- 别名记录 CNAME(Canonical Name)
- 邮件交换主机 MX(Mail Exchange)
- 指针 PTR(Pointer)

4. 添加主机记录

为了使 DNS 服务器能够顺利解析客户的解析请求，就必须将主机的相关数据添加到 DNS 服务器内。下面以任务实例来讲述如何在正向解析区域内建立正向记录。

例如，在正向区域中添加主机记录，解析 www.myserver.net 为 192.168.1.5。

其操作步骤为：

(1) 在 DNS 管理器中，右击要添加主机记录的正向查找区域中的 myserver.net，弹出如图 3-18 所示的快捷菜单。

(2) 选择“新建主机”命令，弹出如图 3-19 所示的“新建主机”对话框。首先在“名称(如果为空则使用其父域名称)”文本框中输入主机名称，则“完全合格的域名(FQDN)”文本框中会显示其主机在域中的全名。然后在“IP 地址”文本框中输入此主机域名对应的 IP 地址。

(3) 单击“添加主机”按钮，这样在 DNS 服务器的正向查找区域 myserver.net 中就会增加一条正向解析记录，如图 3-20 所示。

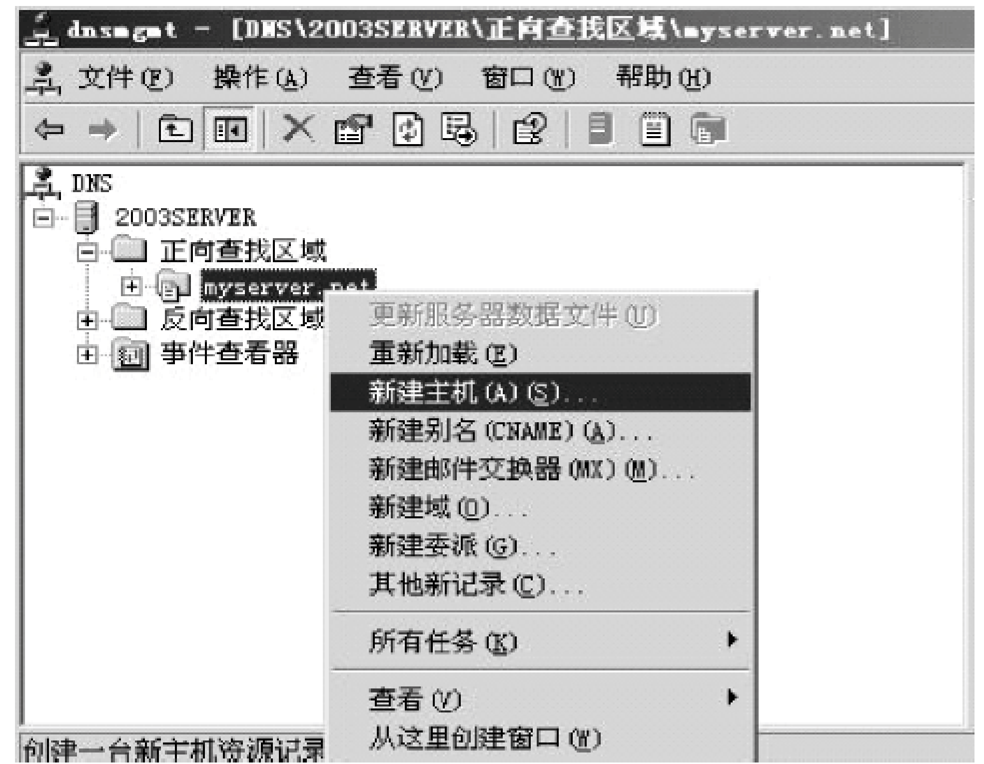


图 3-18 新建主机记录

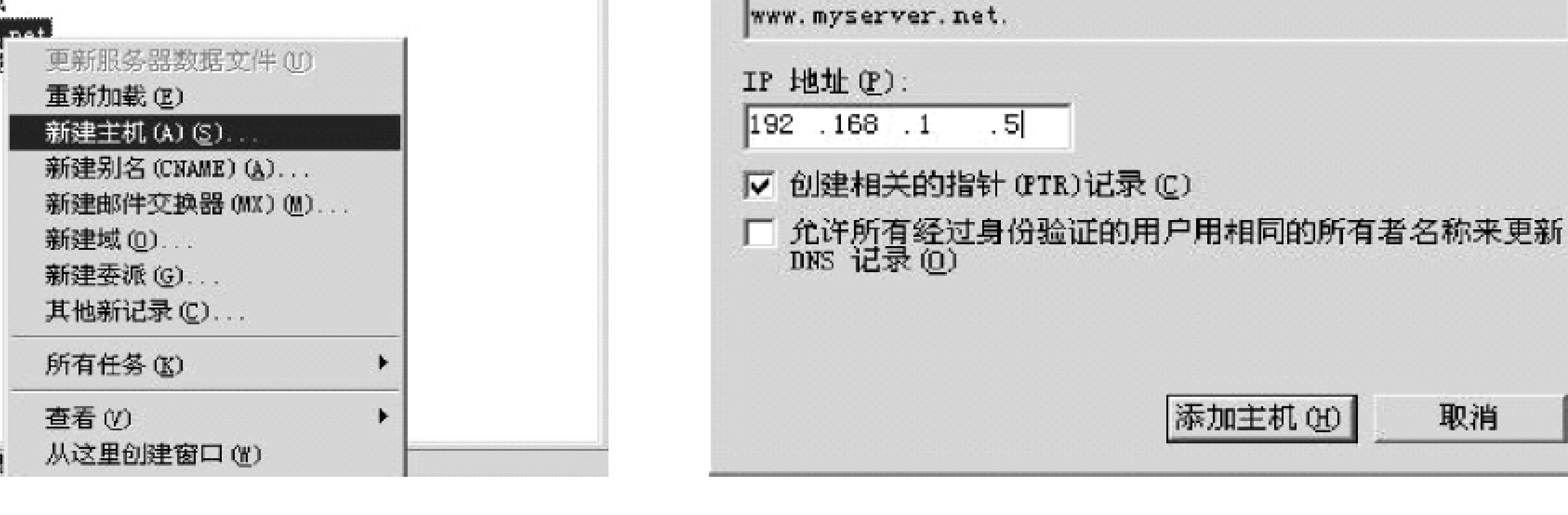


图 3-19 添加 www 主机记录

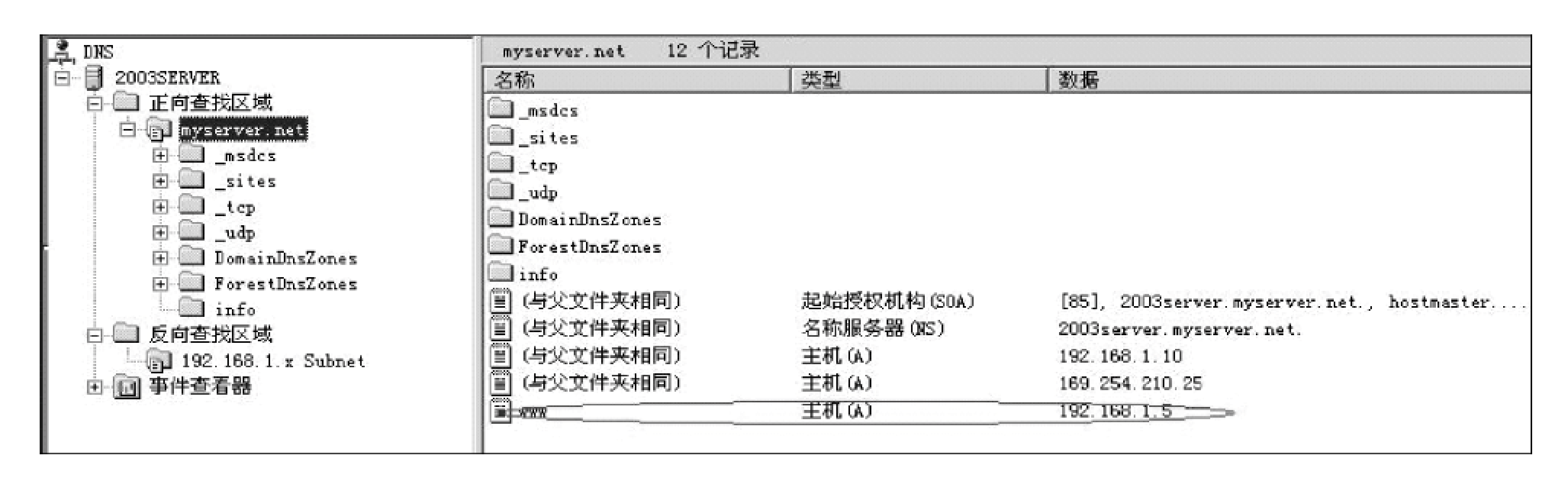


图 3-20 在 DNS 服务器中添加 www.myserver.net 主机记录

5. 添加指针记录

在正反向查找区域中添加指针记录，解析 192.168.1.5 对应为 www.myserver.net。其操作步骤为：

(1) 在 DNS 管理器中，右击反向查找区域中的 192.168.1.x.Subnet 区域，弹出如图 3-21 所示的快捷菜单。

(2) 选择“新建指针”命令，弹出如图 3-22 所示的“新建资源记录”对话框。

由于本例是在域中进行资源记录的创建，所以 IP 地址的网段由反向域的网段信息所决定。在“主机名”文本框中输入此 IP 地址对应的域名全称 www.myserver.net。如果其对应的域名已存在或为了避免错误和冲突可单击“浏览”按钮，弹出如图 3-23 所示的“浏览”对话框，在已设定的正向查找区域的记录中选择其对应的主机名称。然后单击“确定”按钮，则 DNS 服务器的反向查找区域中会产生一条资源记录，如图 3-24 所示。

6. 添加别名主机记录

在正向查找区域中添加一个与 2003server.myserver.net 指向同一个 IP 地址的别名 dns.myserver.net。

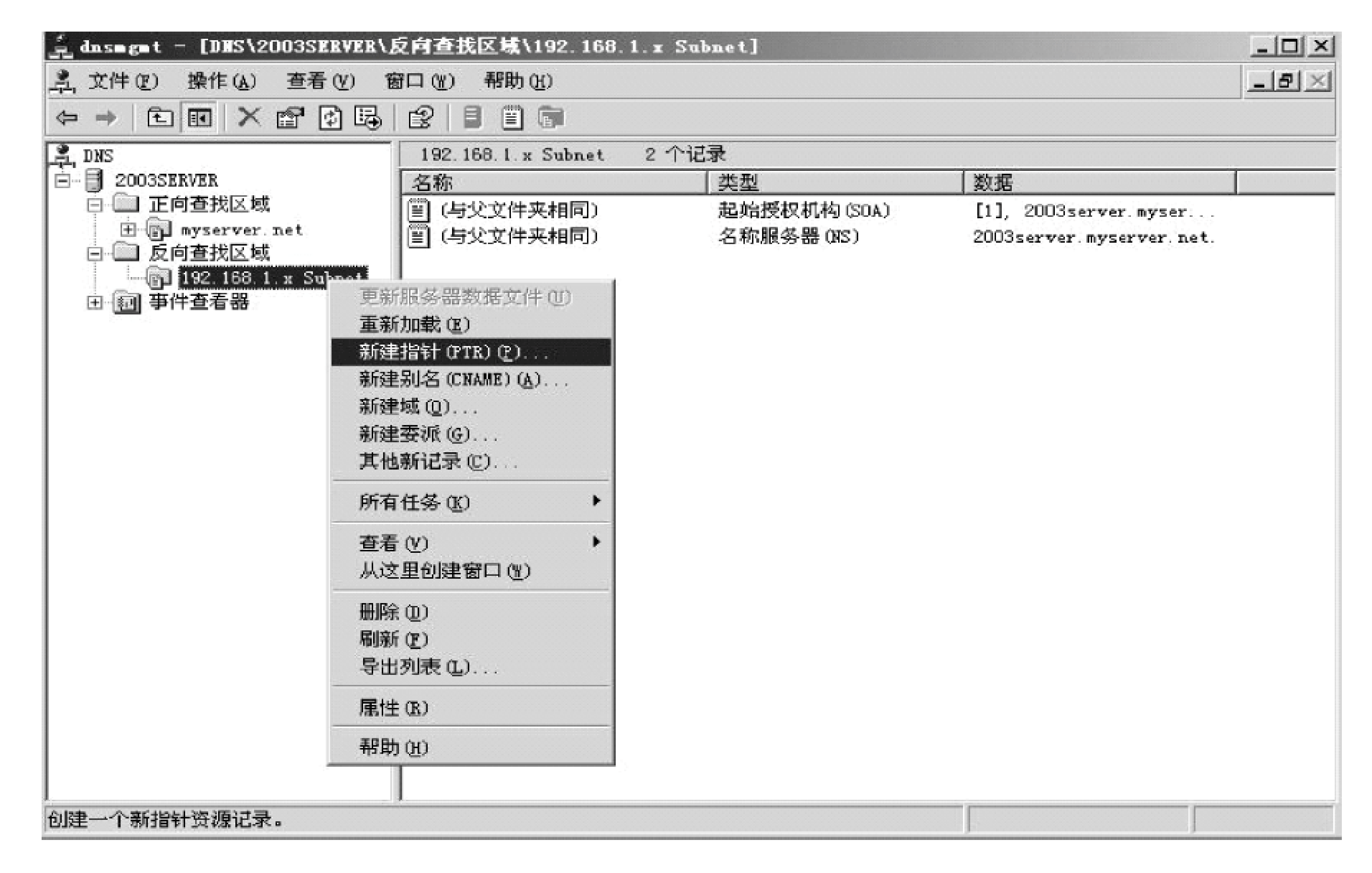


图 3-21　新建反向查找区域的指针记录

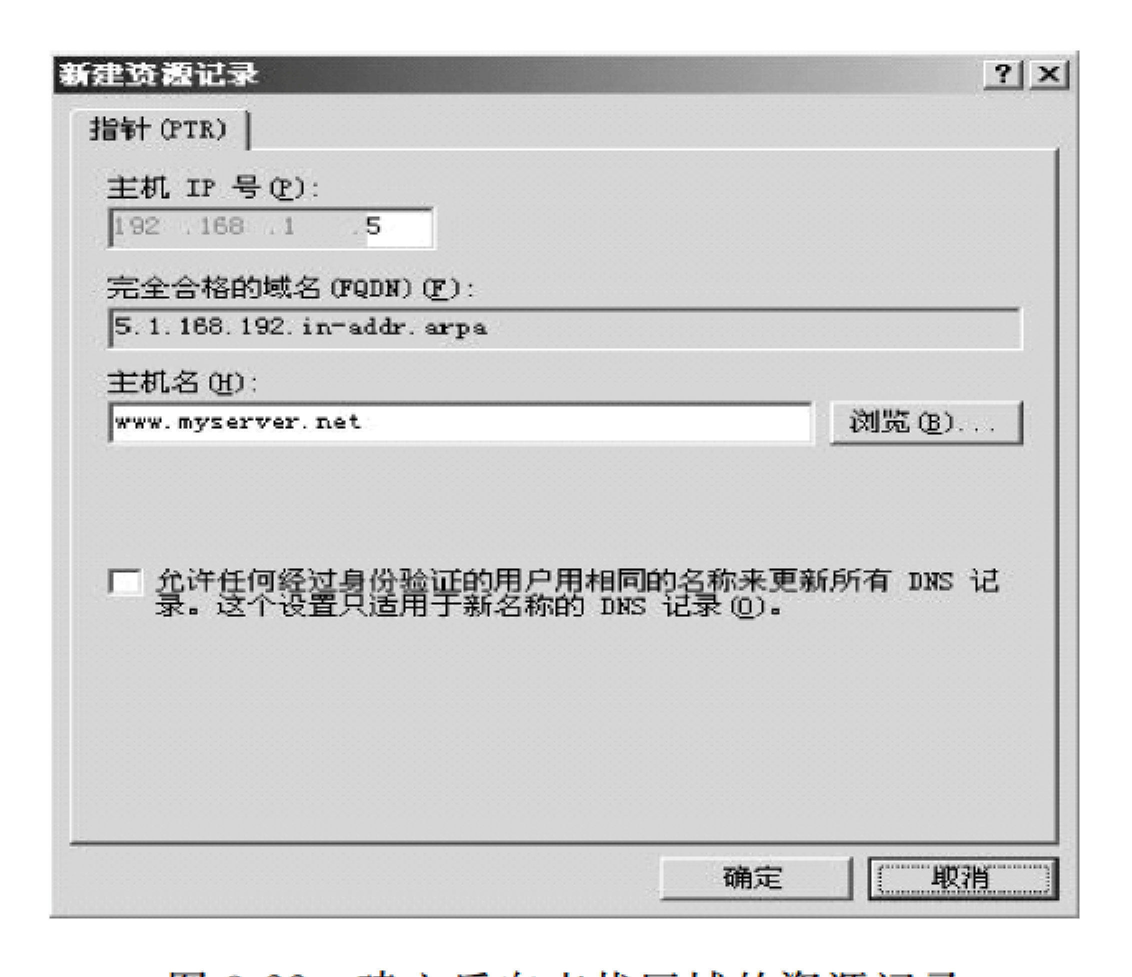


图 3-22　建立反向查找区域的资源记录



图 3-23　选择域名

其操作步骤为：

(1) 在图 3-25 所示的“正向查找区域”上右击，弹出快捷菜单，选择“新建别名”命令，弹出如图 3-26 所示的对话框。

首先在“别名(如果为空则使用其父域)”文本框中输入在本域中的主机别名，在“完全合格的域名(FQDN)”文本框中会显示其最终的域名称。然后在“目标主机的完全合格的域名(FQDN)”文本框中输入此别名指向的主机域名。

(2) 单击“确定”按钮完成别名主机记录的添加，如图 3-27 所示。

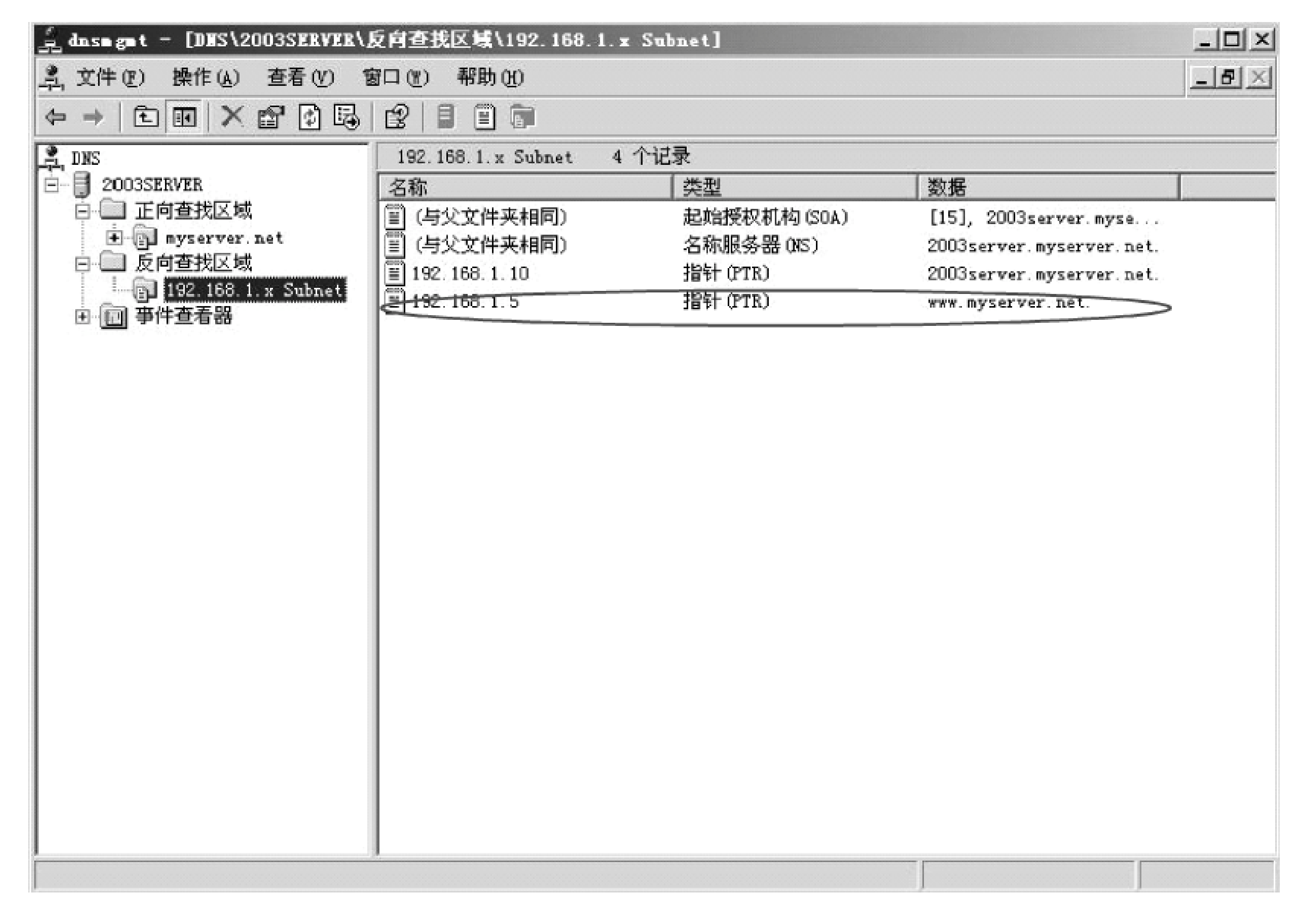


图 3-24　反向区域的资源记录



图 3-25　新建别名主机

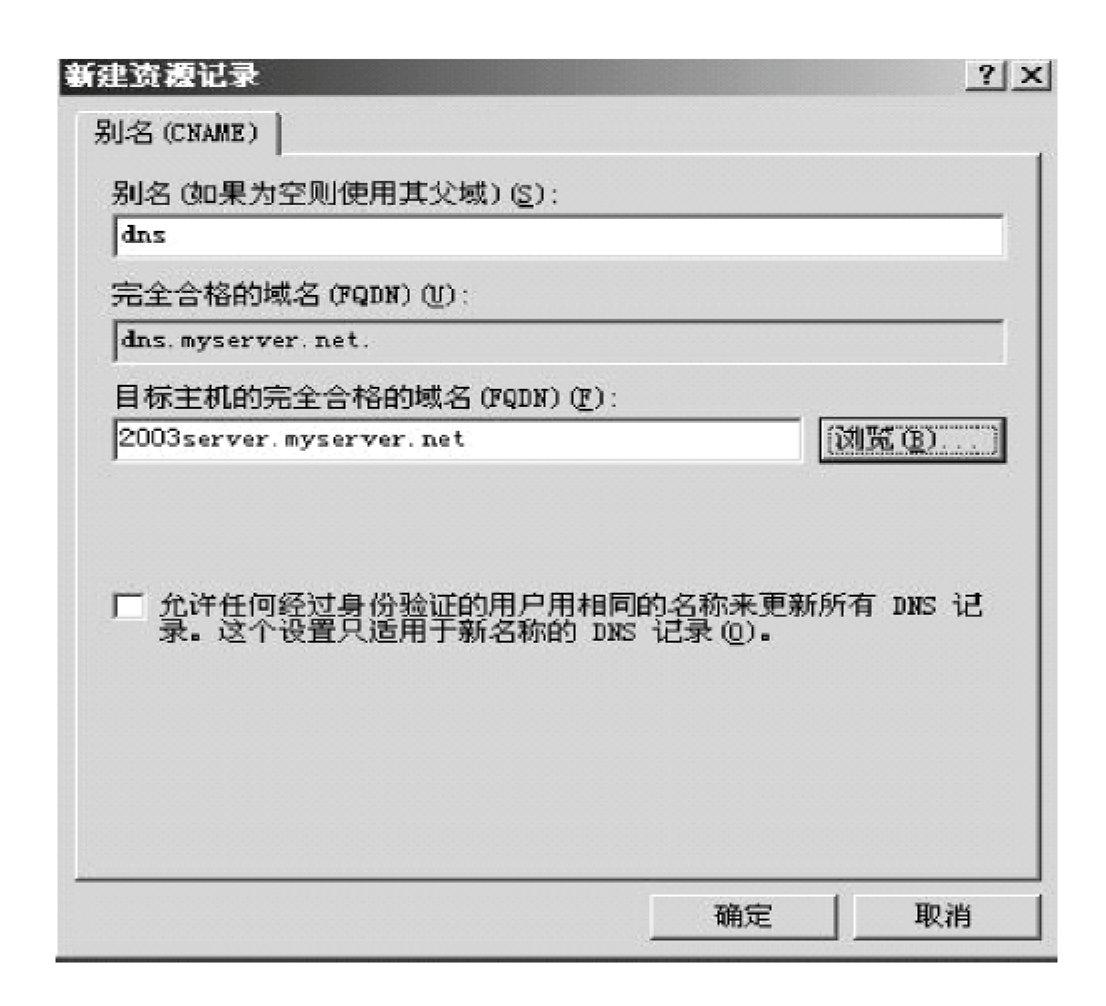


图 3-26　新建别名的资源记录

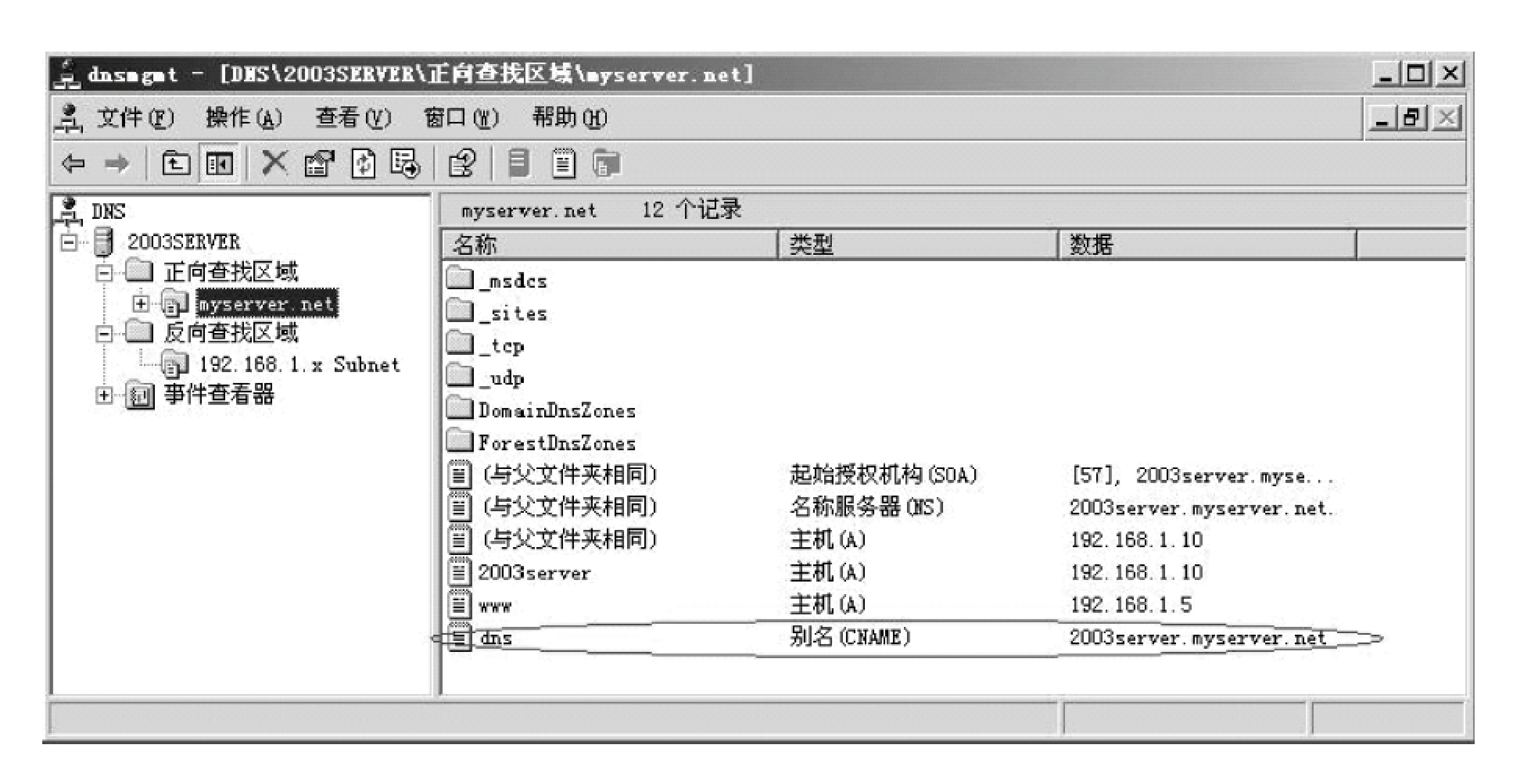
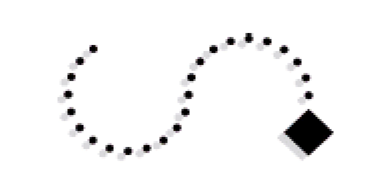


图 3-27　在 DNS 服务器中添加别名主机记录

3.1.4　DNS 测试

当一台服务器的 DNS 设置完毕后，要检测服务器是否正常工作。常用的方法是利用专用工具软件程序 Nslookup。Nslookup 是 Windows 系统自带的程序，它是一个 Win32 应用程序。启动方法为：单击“开始”菜单，选择“运行”命令，在弹出的对话框中输入命令 nslookup，单击“确定”按钮就启动了 DNS 的检测程序。在提示符“>”后面输入要测试的域名或 IP 地址。

（1）测试域名 www.myserver.net，若 DNS 的正向查找区域中有此域名的对应记录，则会显示如下信息：




```
> www.myserver.net
Server：2003server.myserver.net
Address：192.168.1.10

Name：www.myserver.net
Address：192.168.1.10
```

通过此返回信息可以知道，本域名所使用的域名服务器为 2003server.myserver.net，域名服务器的 IP 地址为 192.168.1.10，域名 www.myserver.net 对应的 IP 地址为 192.168.1.10。

(2) 测试 IP 地址 192.168.1.6，若 DNS 的反向查找区域中有此域名的对应记录，则会显示如下信息：

```
> 192.168.1.6
Server：2003server.myserver.net
Address：192.168.1.10

Name：ftp.myserver.net
Address：192.168.1.6
```

通过测试结果可以看出，反向查找区域中有一条记录，它对应的域名为 ftp.myserver.net，对应的 IP 地址为 192.168.1.6。

(3) 测试 IP 地址 192.168.1.5，如果 DNS 的反向查找区域中没有与此 IP 地址对应的域名记录时，则会显示如下信息：

```
> 192.168.1.5
Server：2003server.myserver.net
Address：192.168.1.10

*** 2003server.myserver.net can't find 192.168.1.5：Non-existent domain
```

此信息表明当前 DNS 域名服务器无法解析 192.168.1.5 这个 IP 地址对应的域名。综上所述，就可以根据 Nslookup 测试得出的结论判断是否正确配置 DNS 域名服务器。

3.2 DHCP 服务器的架设

3.2.1 DHCP 的运行方式

DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)是简化主机 IP 地址分配管理协议，是 TCP/IP 协议族中的标准协议之一。DHCP 可以自动将 IP 地址传到请求地址的客户计算机，从而减少人工分配和跟踪分配客户机的 IP 地址所需要的工作量。

3.2.2 DHCP 的工作原理

要使用 DHCP 方式动态分配 IP 地址，要求网络中至少有一台安装了 DHCP 服务的服务器，而且要使用 DHCP 服务的客户端必须具有自动向 DHCP 服务器索取 IP 地址的功能。

当 DHCP 客户机第一次启动时，会自动与 DHCP 服务器通信，并由 DHCP 服务器分

配给 DHCP 客户机一个 IP 地址，直到租约到期，到期后由 DHCP 服务器收回这个 IP 地址，并将其提供给其他 DHCP 客户机使用。

3.2.3 DHCP 服务器的安装与设置

安装 DHCP 服务之前，应做如下准备：

- DHCP 服务器本身应有一个固定的 IP 地址、子网掩码、默认网关等。
- 规划好 DHCP 客户端可以使用的 IP 地址范围。

1. DHCP 的安装

Windows Server 2003 在默认安装时 DHCP 是不进行安装的，所以要使用 DHCP 服务，就要先安装 DHCP 服务。安装步骤如下：

（1）在“控制面板”窗口中双击“添加或删除程序”图标，在弹出的“添加或删除程序”窗口中，选择“添加/删除 Windows 组件”命令。

（2）在弹出的如图 3-28 所示的“Windows 组件向导”对话框中，选择“网络服务”复选框，并单击“详细信息”按钮，弹出如图 3-29 所示的“网络服务”对话框。

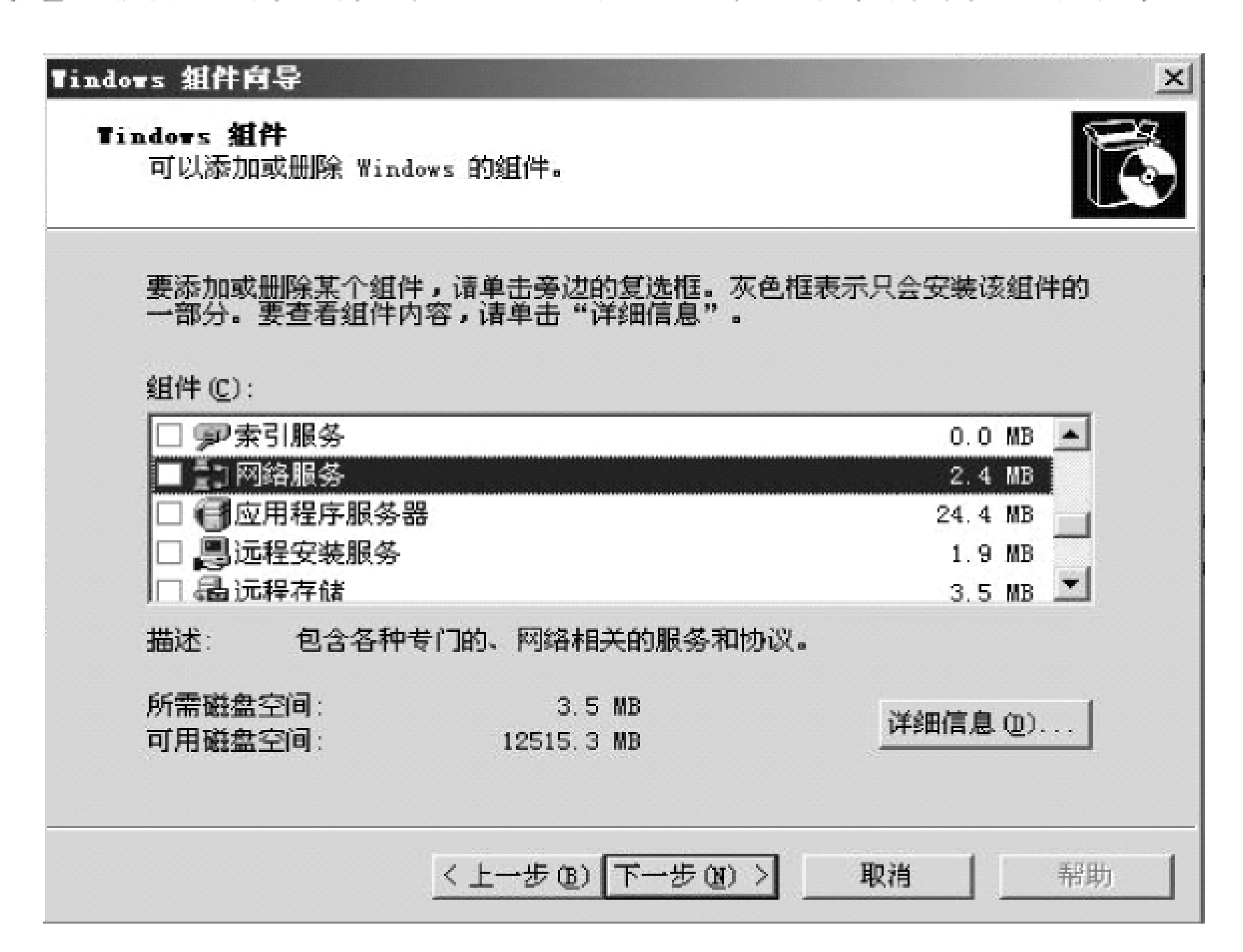


图 3-28　选择网络服务

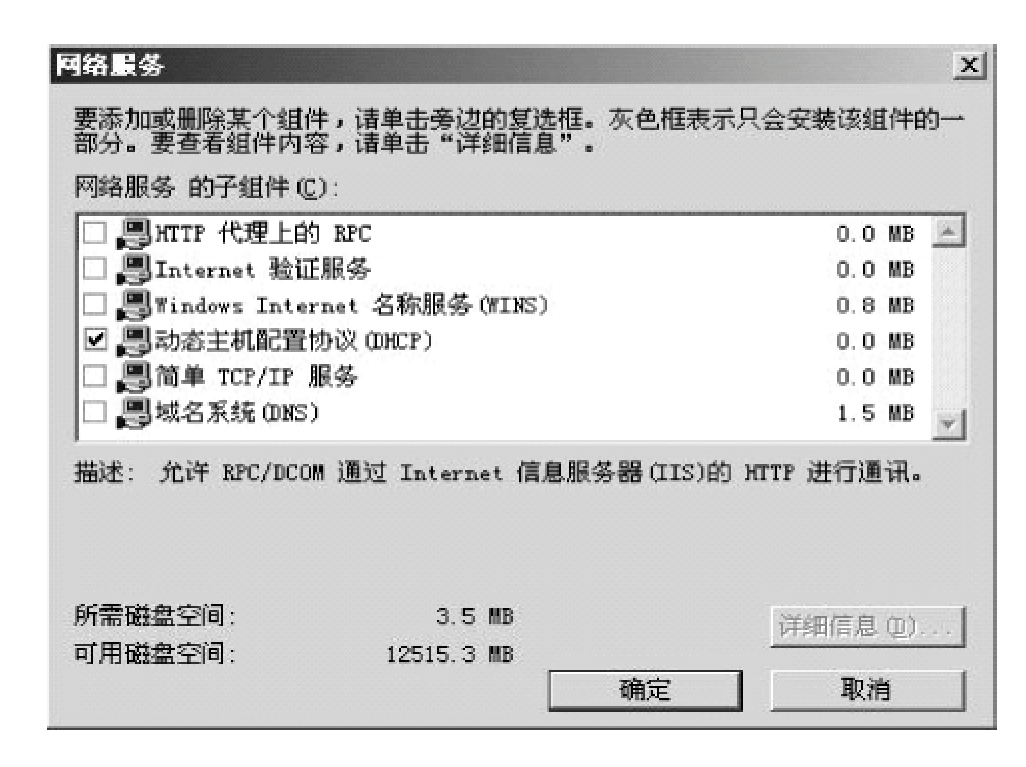


图 3-29　“网络服务”对话框

（3）选择“动态主机配置协议（DHCP）”复选框，单击“确定”按钮，返回“Windows 组件向导”对话框，并单击“下一步”按钮。系统复制文件后，进行服务组件的添加。

（4）安装完毕，选择“开始”→“程序”→“管理工具”→DHCP 命令，对用户和 DHCP 服务器进行设置与管理。

2. 授权操作

在 Windows Server 2003 中，DHCP 服务器安装后不能直接使用，还需要进行授权操作，未经授权的服务器无法提供 DHCP 服务。另外被授权的 DHCP 服务器必须是 AD 中的组成员，否则无法完成授权。对 DHCP 授权操作步骤如下：

（1）选择“开始”→“程序”→“管理工具”→DHCP 命令，打开如图 3-30 所示的 DHCP 窗口。

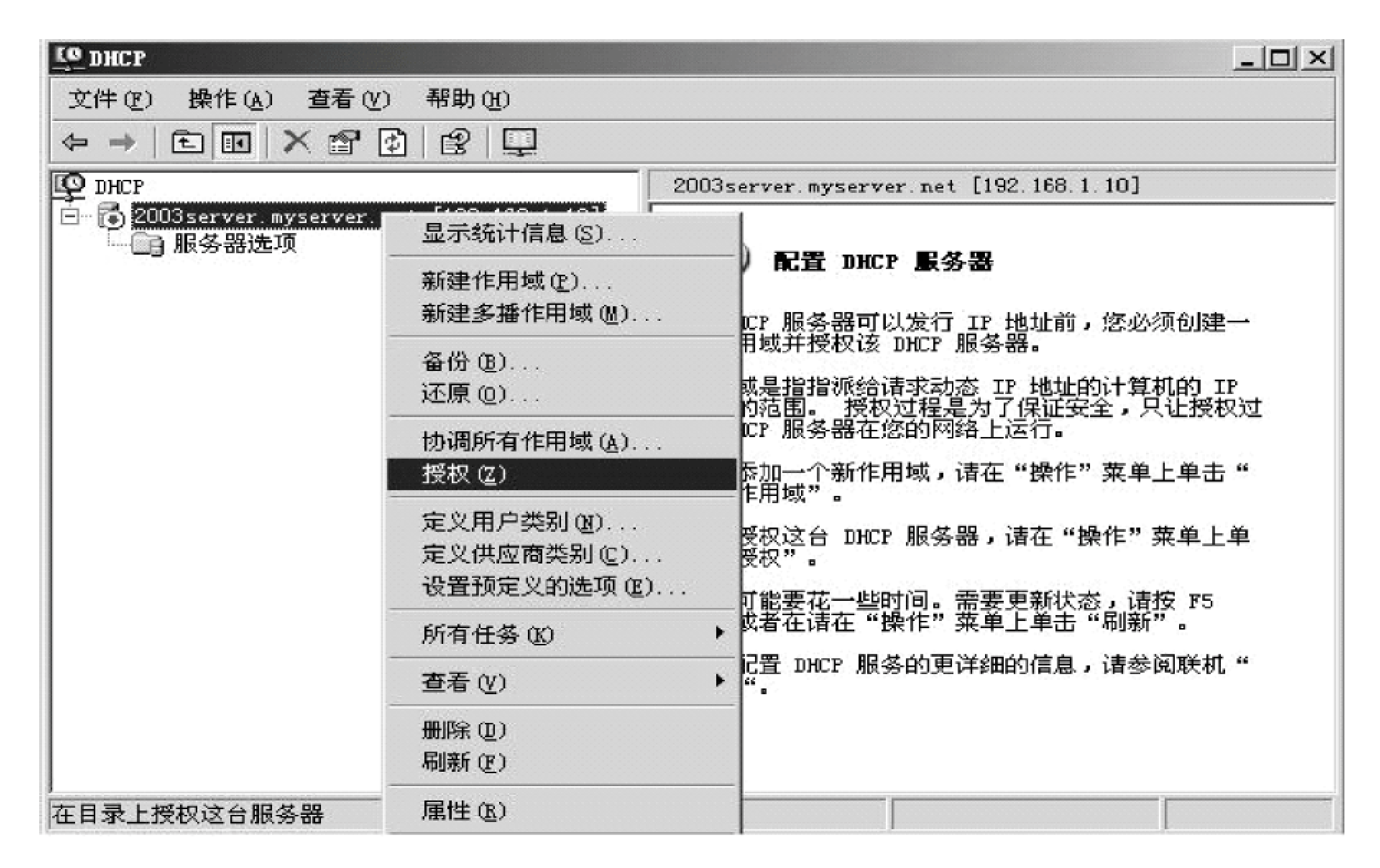


图 3-30　授权启动 HDCP 服务

（2）在 DHCP 窗口中，右击服务器名称 2003server. myserver. net[192. 168. 1. 10]，在弹出的快捷菜单中选择“授权”命令。这样 DHCP 服务才真正开始工作。

3. 新建作用域

在 myserver. net 域中新建一个动态地址分配区域，起始 IP 地址为 192. 168. 1. 100，终止 IP 地址为 192. 168. 1. 200，子网掩码为 255. 255. 255. 0。

操作步骤为：

（1）右击 DHCP 服务器的名字，在弹出的快捷菜单中选择“新建作用域”命令。

（2）在弹出的对话框的“名称”文本框中输入作用域的域名称 myserver. net，如图 3-31 所示。

（3）单击“下一步”按钮，在弹出的对话框中输入当前 DHCP 可以动态分配的 IP 地址范围、子网掩码长度及子网掩码值，如图 3-32 所示。

新建作用域向导
作用域名
您必须提供一个用于识别的作用域名称。您还可以提供一个描述（可选）。
为此作用域输入名称和描述。此信息帮助您快速标识此作用域在网络上的作用。
名称(A): myserver.net
描述(D):
< 上一步(B) 下一步(N) > 取消

图 3-31　输入作用域名称

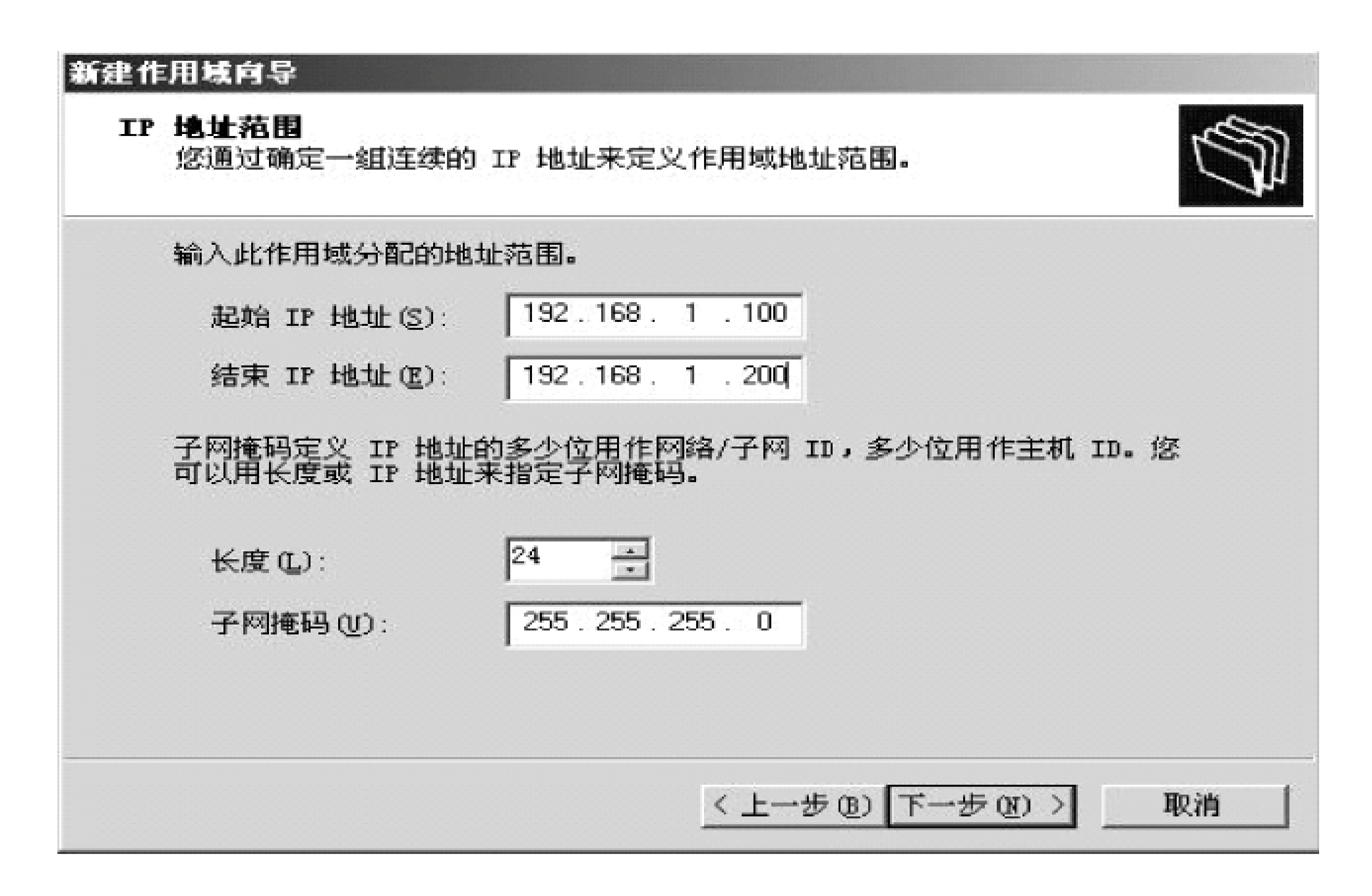
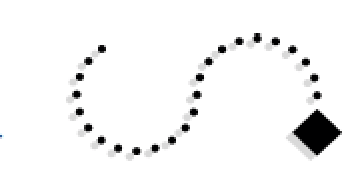


图 3-32　设置 DHCP 分配的动态 IP 地址范围

(4) 单击“下一步”按钮，弹出如图 3-33 所示的对话框。在此对话框中，可以设置 DHCP 动态分配的 IP 范围中某些地址可以排除在外，不会分配给其他主机，这样可以让一些 IP 地址成为私有，为其他的服务器或主机预留可分配使用的地址。如果分配的动态 IP 地址范围中没有希望预留的，此项可以不设置。

(5) 单击“下一步”按钮，弹出如图 3-34 所示的对话框。在这个对话框中，可以设置服务器分配的作用域租约期限。默认的最大租用期限为 8 天，用户可以根据当前域中主机的特点和使用的时间长短来进行设置。一般情况下，如果要分配使用 IP 地址的多为移动设备，可以设置租期相对短些，这样 IP 地址的使用频度会增加，有利于更多的主机进行对网络连接的需求。如果要分配使用 IP 地址的多为固定设备，用户寻求的是长期可用，故可设置其租期相对长些。



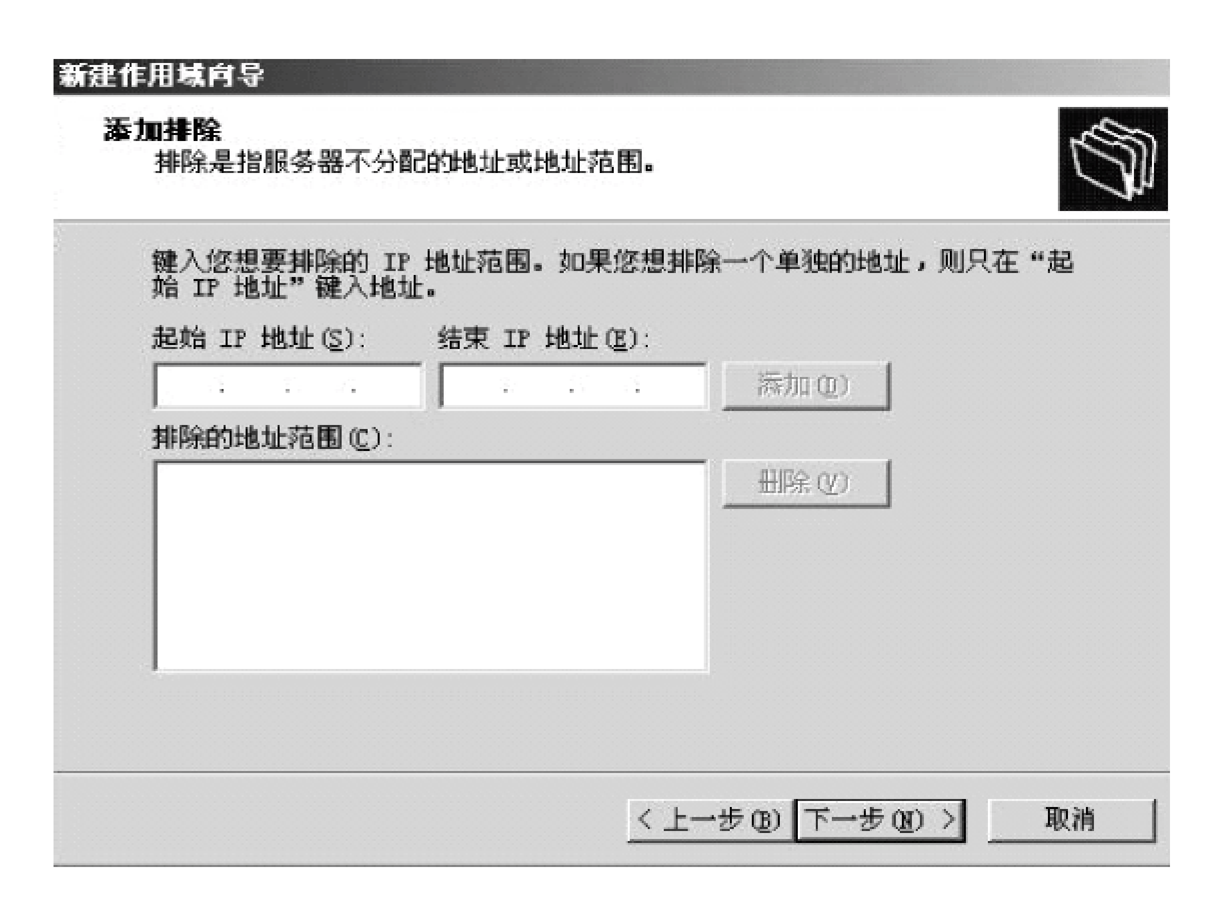


图 3-33　设置排除的地址范围

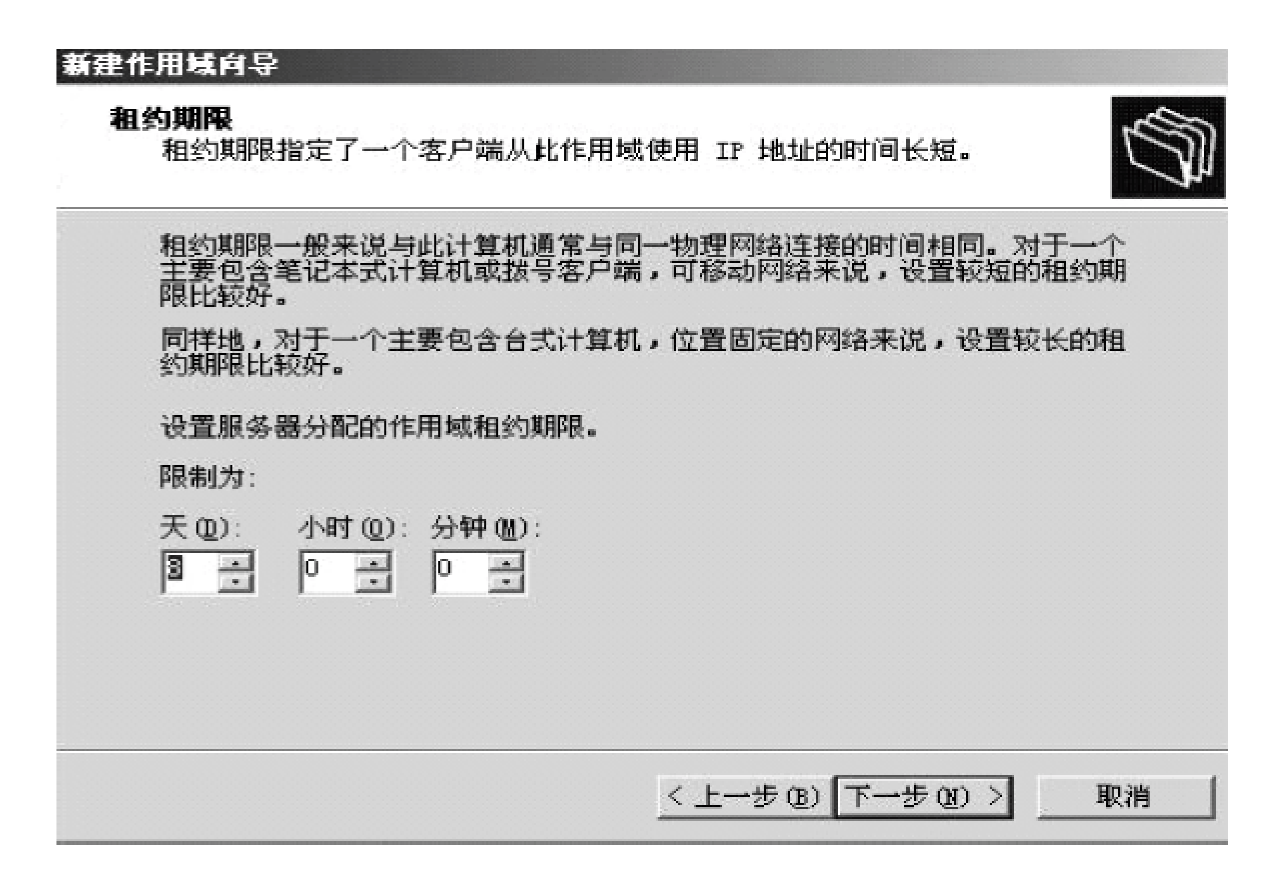
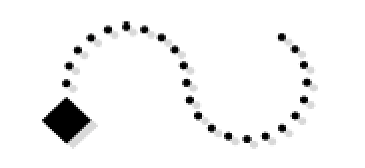


图 3-34　设置客户端申请地址的使用租期

(6) 单击“下一步”按钮，弹出如图 3-35 所示的对话框。在该对话框中，可以指定分配的主机使用的网关，在“IP 地址”文本框中输入一个网关地址，单击“添加”按钮，将网关地址加入到设置中去。若分配的 IP 地址范围所在的域没有外网连接，也可以直接单击“下一步”按钮。

(7) 单击“下一步”按钮，弹出如图 3-36 所示的对话框。在该对话框中，可以配置 DHCP 其他选项。如果立即对 DHCP 其他选项进行设置，选择“是，我想现在配置这些选项”单选按钮，并单击“下一步”按钮对 DHCP 其他选项，如 WINS、DNS 等进行设置。如果不马上进行配置，选择“否，我想稍后配置这些选项”单选按钮，可以跳过 DHCP 其他选项的设置。

(8) 单击“下一步”按钮，弹出如图 3-37 所示的对话框，单击“完成”按钮，完成整个 DHCP 区域的基本设置。



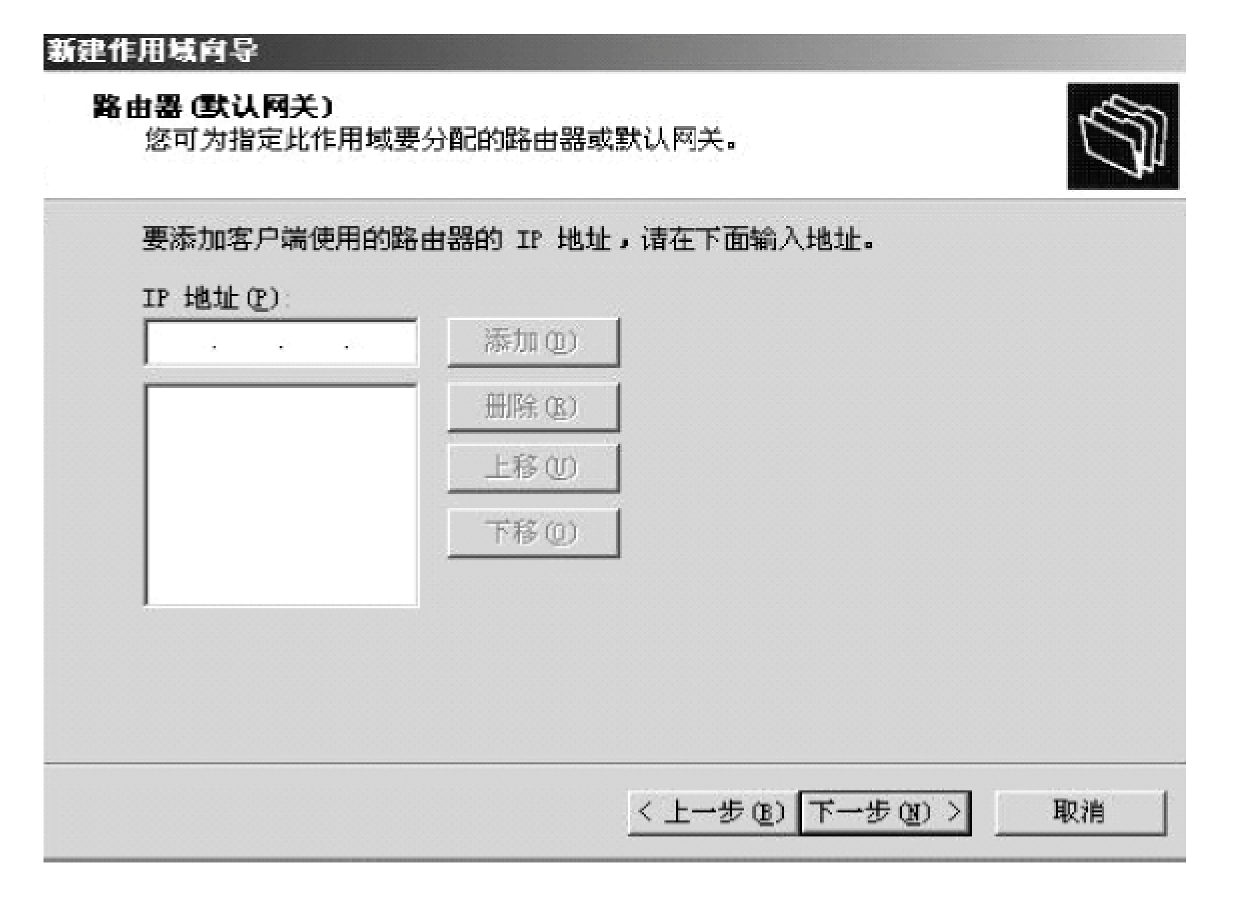


图 3-35　指定路由器或默认网关

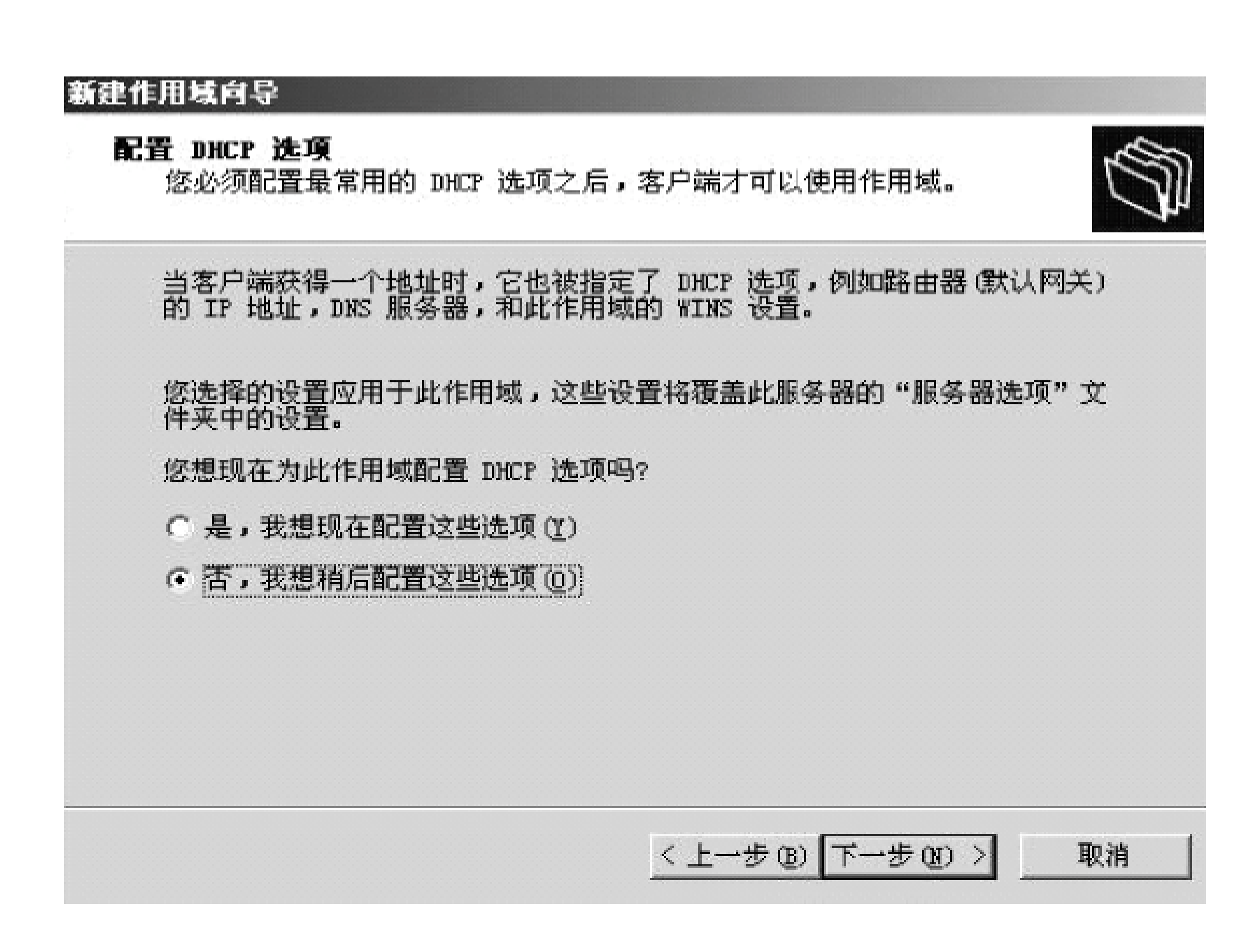


图 3-36　DHCP 其他选项的设置

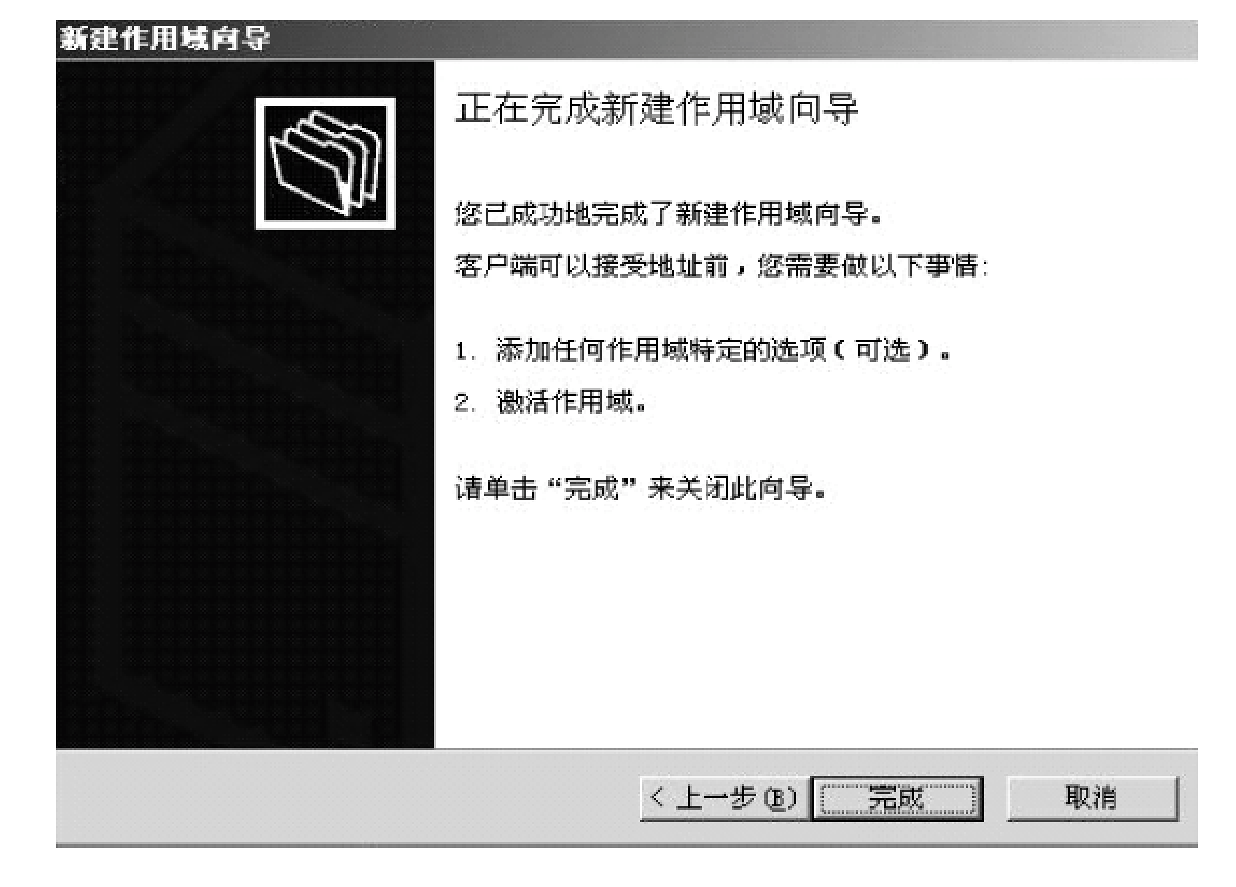
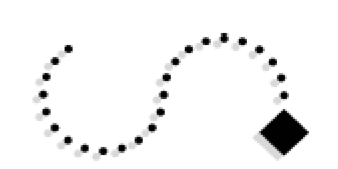


图 3-37　完成 DHCP 的设置



至此，一个基本的 DHCP 服务器配置完成。DHCP 服务器能够为用户所在的物理连接网络提供 IP 地址的自动分配，使每一台计算机都能和其他计算机进行通信，并且互不影响。

4. DHCP 属性的设置

DHCP 新建作用域设置完毕，可以对其属性进行设置。操作步骤如下：

(1) 在 DHCP 服务器 2003server. myserver. net[192. 168. 1. 0]的"作用域"上右击，弹出如图 3-38 所示的快捷菜单，选择"属性"命令，进行属性设置。



图 3-38　作用域的属性设置

(2) 在弹出的"作用域[192. 168. 1. 0]myserver. net 属性"对话框中有 3 个选项卡，可以对已经设置的 DHCP 属性进行更改。

① 在"常规"选项卡中可以对作用域的域名、地址范围、租约期限进行相应的更改，如图 3-39 所示。

② 在 DNS 选项卡中可以设置 DHCP 与 DNS 的对应，还可以设置 DNS 的记录内容，如图 3-40 所示。



图 3-39　"常规"选项卡

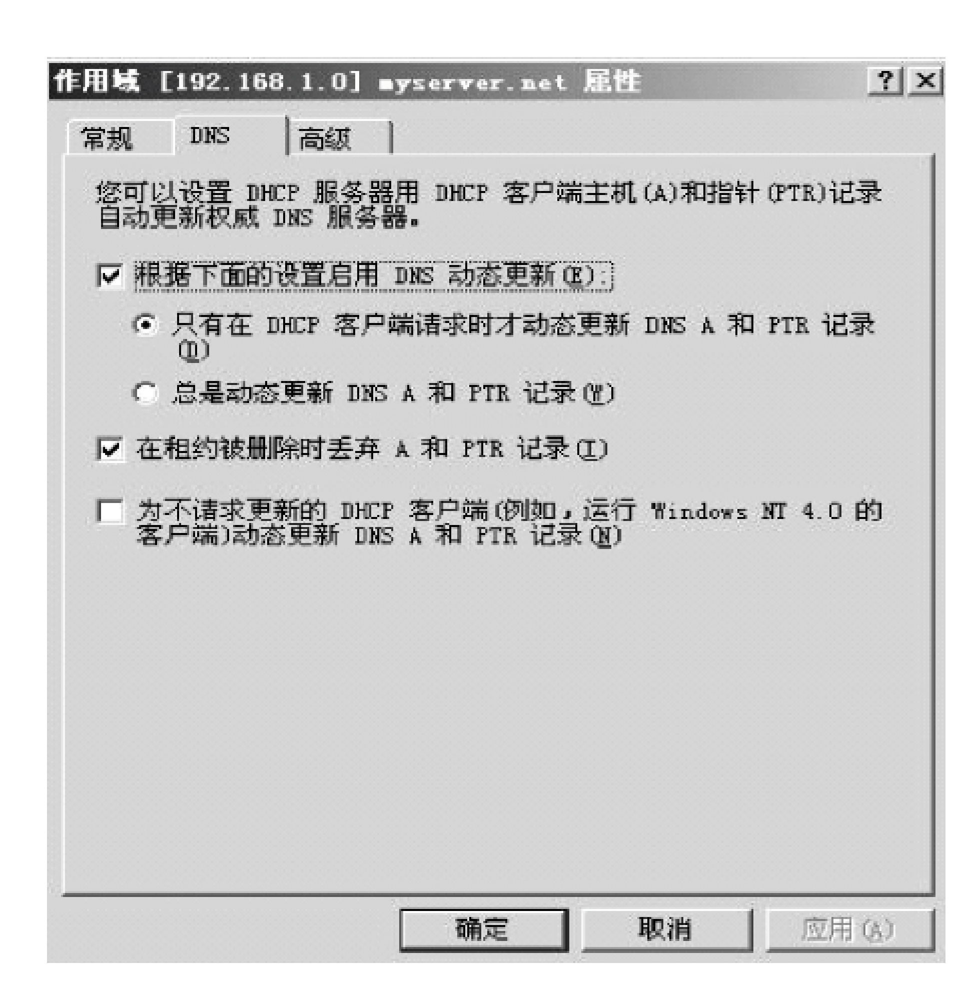


图 3-40　DNS 选项卡



③ 在“高级”选项卡中可以为其他具有动态主机地址分配功能的客户端选择分配的策略，还可以对 DHCP 客户端的租约期限进行设置，如图 3-41 所示。

(3) 设置完成后，单击“确定”按钮，完成 DHCP 属性的设置。

DHCP 服务器配置完毕，在网络中的客户端主机要想自动获取 IP 地址的 DHCP 服务，还需要进行客户端设置。

5. DHCP 客户端配置

以 Windows XP 为客户端对象进行配置。操作步骤如下：

(1) 在客户端主机桌面上，右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，在弹出的“网络连接”窗口中，右击“本地连接”图标，在弹出的快捷菜单中选择“属性”命令。

(2) 弹出“本地连接 属性”对话框，双击“Internet 协议(TCP/IP)”，弹出“Internet 协议(TCP/IP)属性”对话框。选中“自动获得 IP 地址”和“自动获得 DNS 服务器地址”单选按钮，如图 3-42 所示。



图 3-41 “高级”选项卡

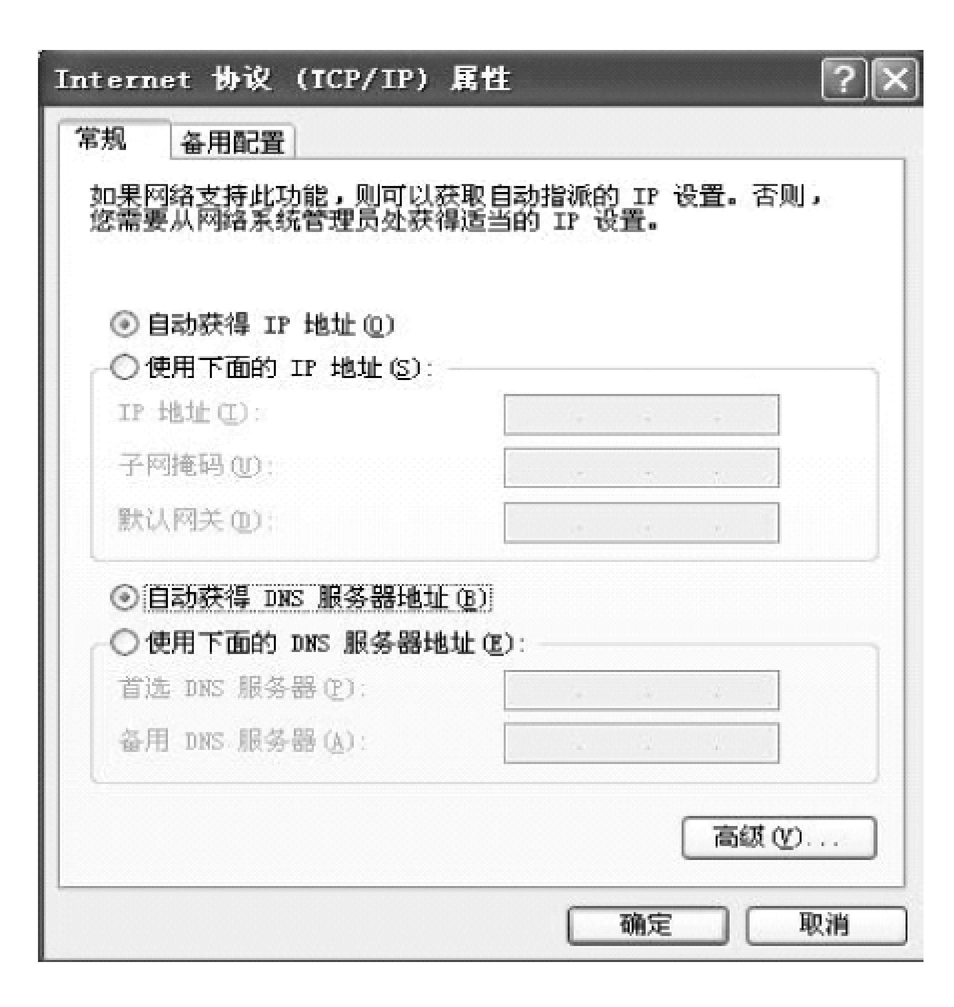


图 3-42 DHCP 客户端设置

(3) 单击“确定”按钮，这样客户端的主机就能够利用 DHCP 服务器自动提供的 IP 地址进行网络访问。

3.3 IIS 的使用

3.3.1 IIS 的介绍

IIS(Internet Information Services)也称为 Internet 信息服务，包括 Web、FTP 和 SMTP 服务器 3 个基本功能，可以为局域网实现内部的 Internet 信息服务，也可使内部网连接到 Internet 上，实现远程信息服务。IIS 主要的功能是提供用户创建 Web 站点的服

务。Windows Server 2003 使用了 IIS 6.0,较以前版本在功能上有了很大的提高,其特点为:

(1) 可靠性。IIS 6.0 的请求处理结构提供一个应用程序来隔离环境,使单个 Web 应用程序能够在其各自的、自我包含的工作进程中运行,因此比早期版本更可靠。

(2) 安全性。IIS 6.0 包括各种可确保网站和 FTP 站点内容以及通过站点传输的数据的完整性的安全性功能和技术。IIS 6.0 安全功能包括:身份验证、访问控制、加密、证书和审核。

(3) 性能强。新一代应用程序对 Web 服务器的性能和可伸缩性提出了更高的要求。如果增加 HTTP 请求的处理速度并允许在一个服务器上运行更多的应用程序和站点,则可以直接减少宿主站点所需的服务器。

(4) 运用了多种 Web 技术。IIS 6.0 使用的 ASP.NET 允许用户充分利用公共语言运行库的功能,例如,类型安全、继承、语言互操作性和版本控制。IIS 6.0 还为最新的 Web 标准提供支持,例如,XML、简单对象访问协议(SOAP)和 Internet 协议版本 6.0 (IPv6.0)。

(5) 强大的管理能力。为了满足各类客户的需要,IIS 提供各种管理功能和管理工具。管理员可以用 IIS 管理器、管理脚本或通过直接编辑 IIS 纯文本配置文件来配置运行 IIS 6.0 的服务器。管理员还可以远程管理 IIS 服务器和站点。

Windows Server 2003 在安装时,如果选择安装 IIS 服务,则系统会自动创建一个默认的 Web 站点和一个 FTP 站点以提供相应的服务。IIS 的安装可以像安装 DNS 和 DHCP 一样,在"添加/删除 Windows 组件"窗口中选择安装相应的 IIS 组件。IIS 安装完成后,系统中会自动添加一个 Internet 信息服务(IIS)管理器。在如图 3-43 所示的"Internet 信息服务(IIS)"对话框 IIS 中可以对 Web、FTP 及 SMTP 服务进行管理。

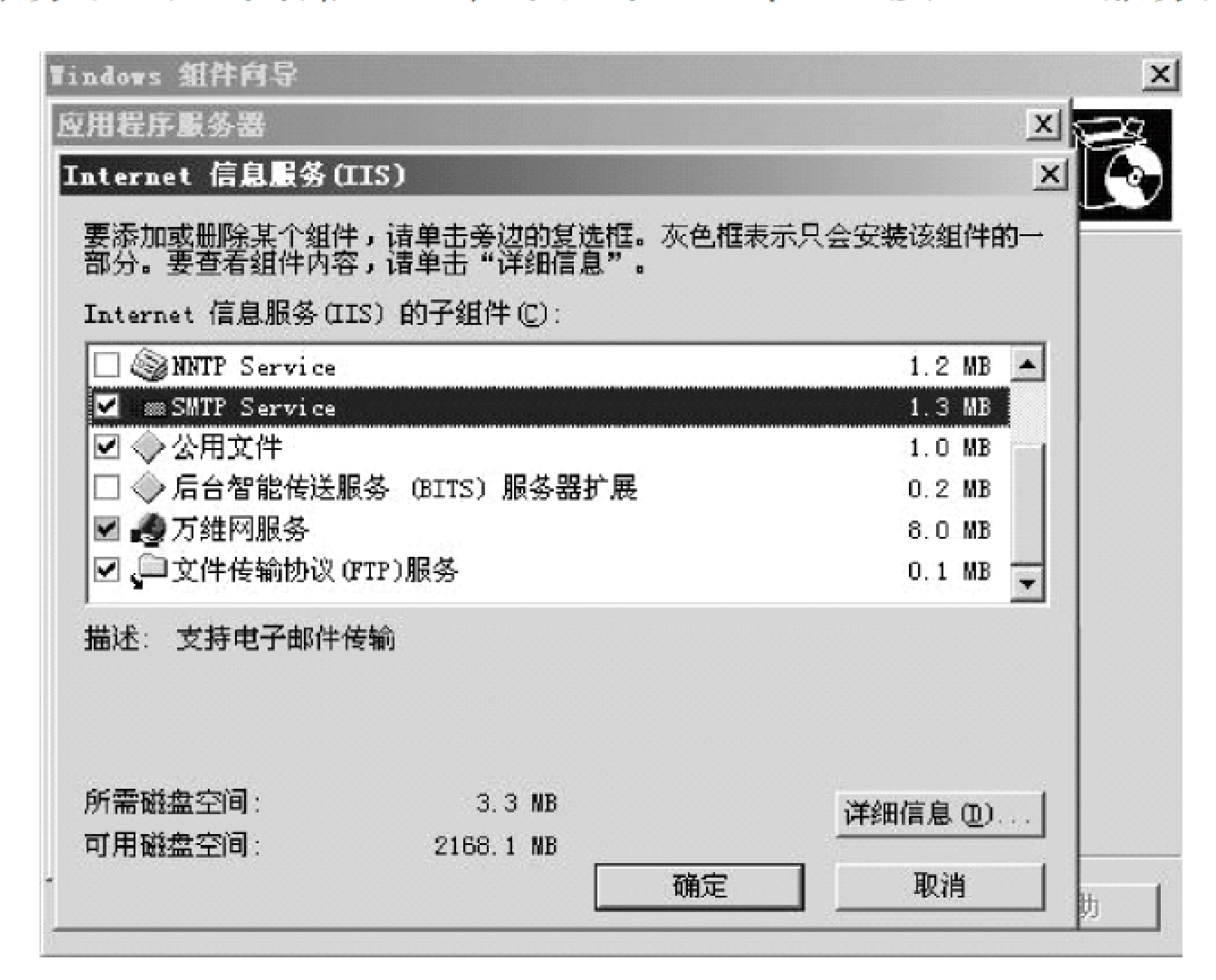


图 3-43 "Internet 信息服务(IIS)"对话框

下面进一步学习在 IIS 中管理 Web 和 FTP 的方法。

3.3.2 Web站点的建立与管理

1. 设置主目录

在 IIS 中,用于向 Internet 发布信息的位置称为主目录或根节点,主要用来设置 Web 站点中网页的主页和一些相关的文件、动画、声音、图像等。用户通过单击主页或相关链接来进一步浏览其他的网页内容。每一个 Web 站点必须有一个主目录。主目录的作用是告诉访问者所有的访问文件的位置,以便进行快速链接。

例如,某站点的 Internet 域名为 www.myserver.net,而主目录为 D:\myserver.net\www,客户端浏览器通过 http://www.myserver.net 可访问 D:\myserver.net\www 目录中的文件。

设置主目录的操作步骤如下:

(1) 打开 IIS 管理器

选择"开始"→"程序"→"管理工具"→"Internet 信息服务(IIS)管理器"命令,弹出"Internet 信息服务(IIS)管理器"窗口,如图 3-44 所示。在这个窗口中,可以进行有关 IIS 的设置。

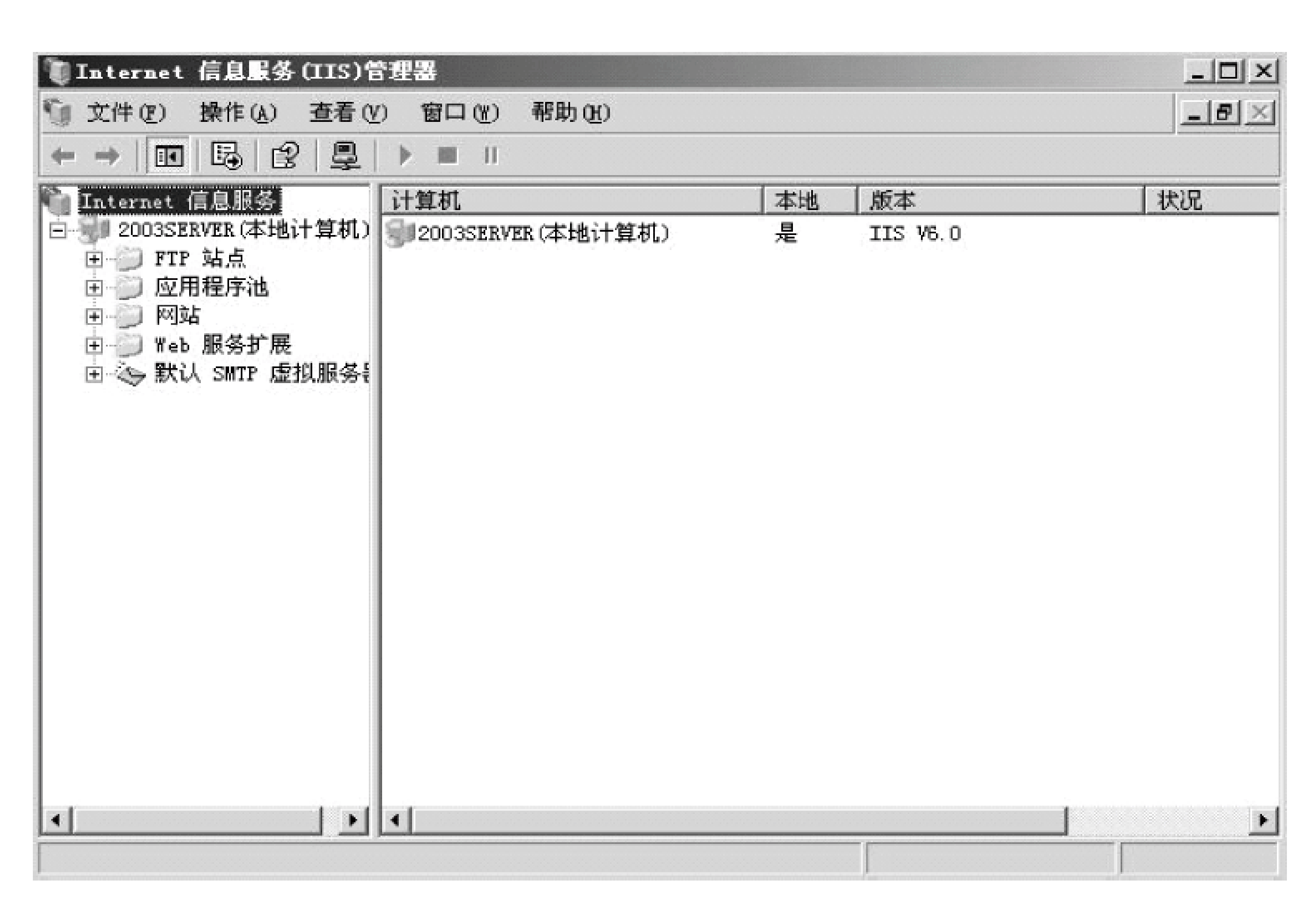
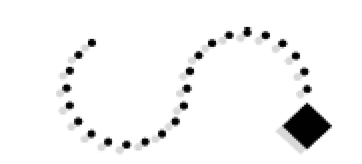


图 3-44 "Internet 信息服务(IIS)管理器"窗口

(2) 设置主目录

在"Internet 信息服务(IIS)管理器"窗口中,单击"网站"节点,在"默认 Web 站点"节点图标上右击,在弹出的快捷菜单中选择"属性"命令。在弹出的"默认网站 属性"对话框中有若干个选项卡,在这些选项卡中可以设置此 Web 站点的所有属性。打开"主目录"选项卡,如图 3-45 所示。

设置 Web 页对应服务器的位置,在"本地路径"文本框中输入相应的位置 D:\myserver.net\www。



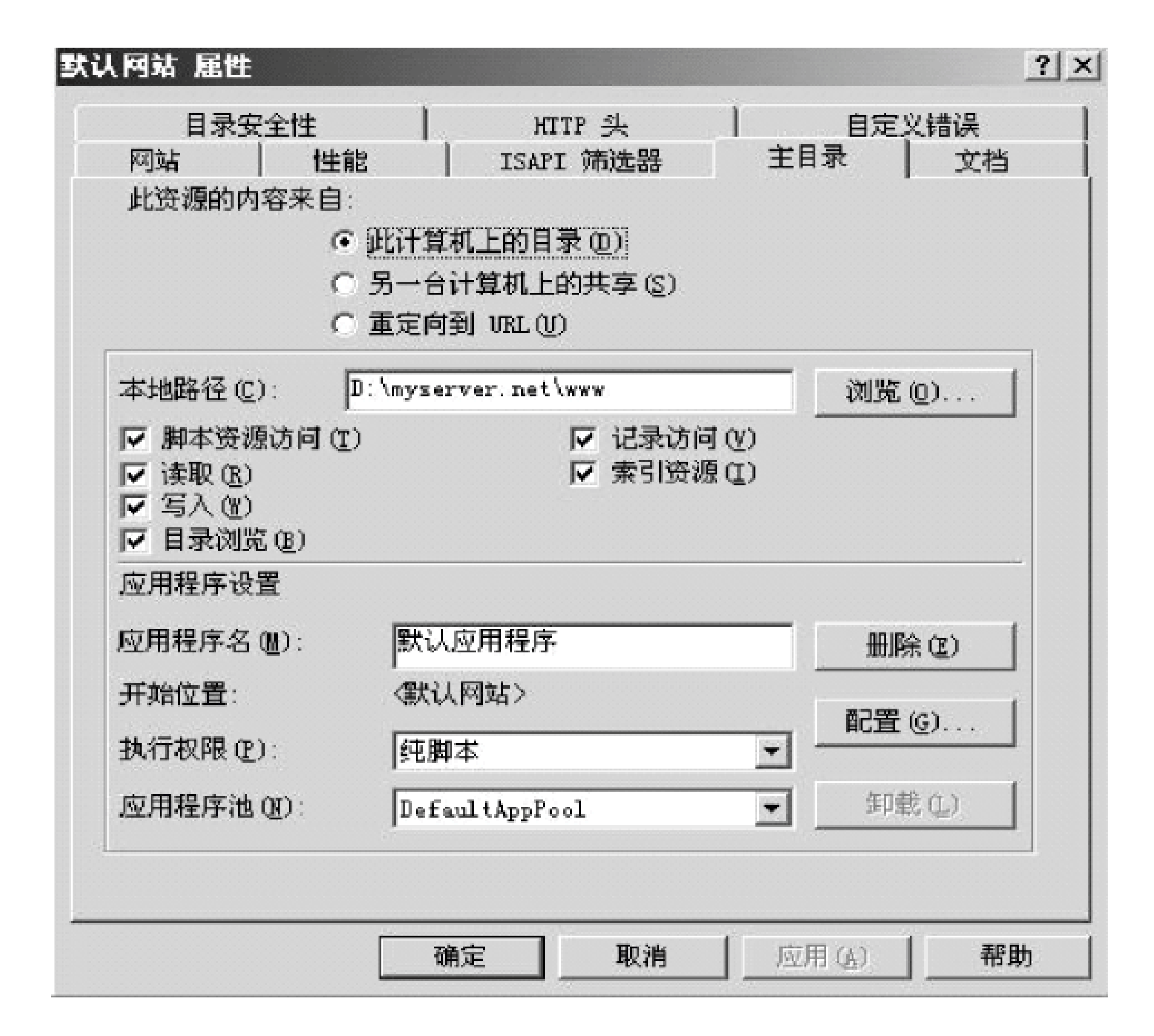


图 3-45　主目录设置

在“此资源的内容来自”选项区域中，有 3 个用来选择主目录内容来源的单选按钮。若资源来自当前服务器的某个目录，应选择“此计算机上的目录”单选按钮；若资源来自其他计算机共享的目录，应选择“另一台计算机上的共享”单选按钮；若资源来自 Internet 上的某个 Web 站点，则应选择“重定向到 URL”单选按钮，并指明 URL 地址。

在对资源路径进行选择后，还要设置与其访问有关的权限。IIS 中对资源的访问权限包括：读取、写入、目录浏览、索引资源、记录访问和脚本资源访问。在主目录中选择相应的权限的复选框，设置对资源的控制权限。

设置主目录的目的是告诉 IIS 服务器其可访问的资源位置和访问权限。设置完毕，单击“确定”按钮应用此设置。

2. 虚拟目录的创建

当一台 IIS 服务器中存放的资源文件不在同一个目录时，为了使用户能够对资源进行统一的访问，就要建立虚拟目录来对不同资源位置进行管理。访问虚拟目录中的文件就像访问主目录中的文件一样，虚拟目录能够实现同主目录相同的功能，但它的物理位置并不在主目录中。

建立一个虚拟目录，必须为虚拟目录规划一个名字，作为 Web 浏览器访问该目录的名称标识。站点管理员可以通过此标识建立 URL 地址与其实际目录的对应关系。

建立一个虚拟目录，别名为 class，实际位置为 C:\class，对应的 URL 地址为 http://www.myserver.net/class。

建立虚拟目录的操作步骤如下：

(1) 在“Internet 信息服务(IIS)管理器”窗口中右击“默认网站”，在弹出的快捷菜单中，选择“新建”→“虚拟目录”命令，如图 3-46 所示。

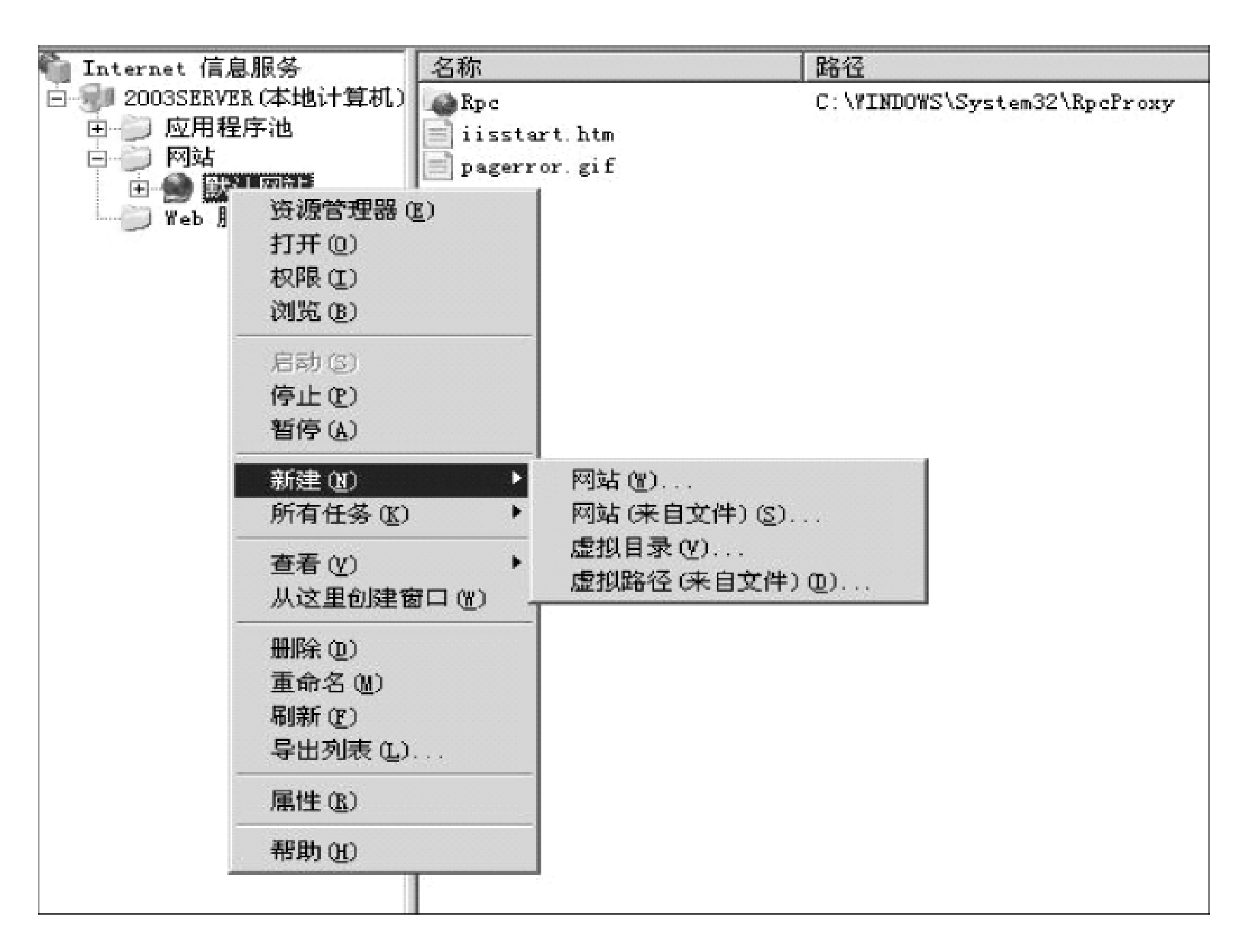


图 3-46　添加虚拟目录

（2）在弹出的"虚拟目录创建向导"对话框中，单击"下一步"按钮，弹出如图 3-47 所示的对话框。在此对话框的"别名"文本框中输入用于识别站点目录的标识别名 class。

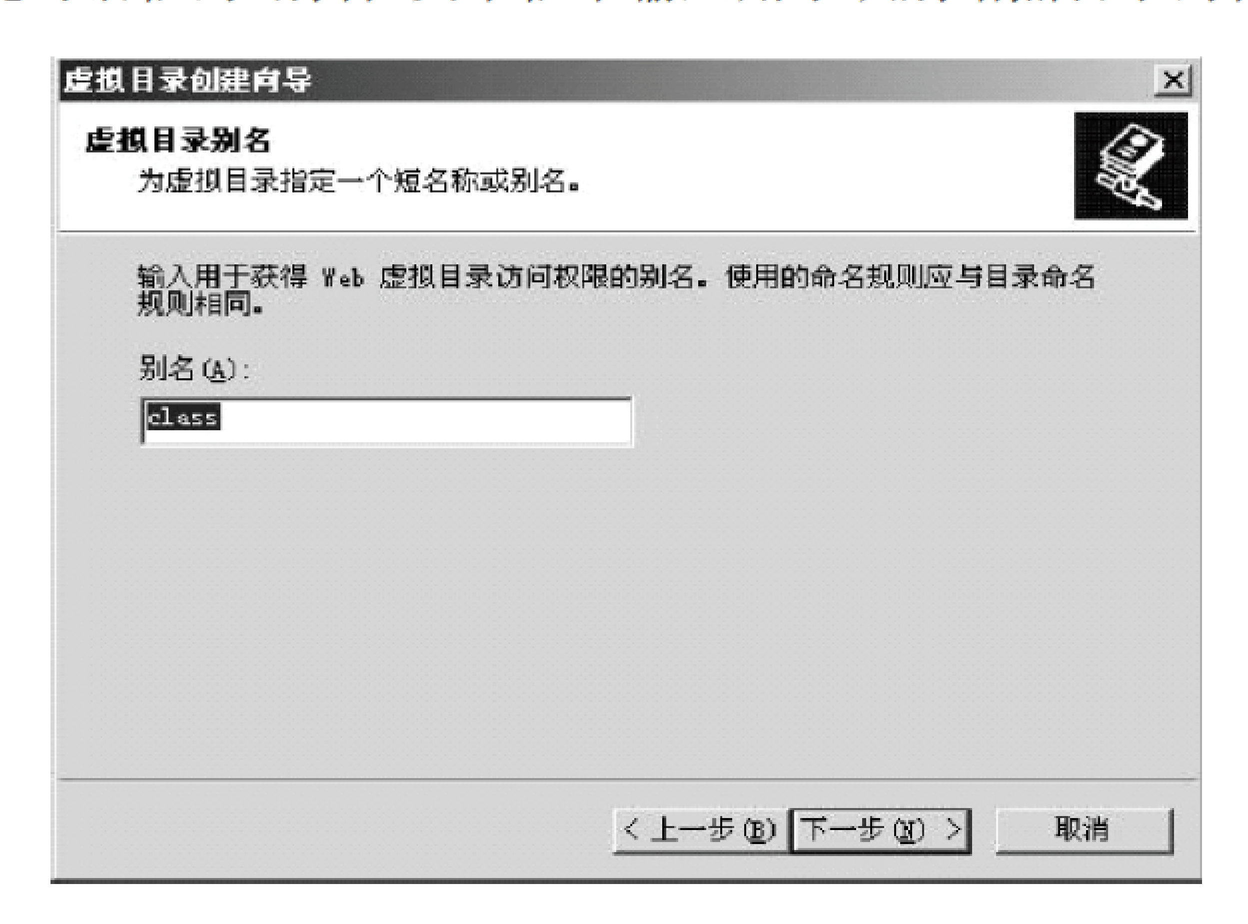


图 3-47　设置虚拟目录的别名

（3）单击"下一步"按钮，弹出如图 3-48 所示的对话框。在此对话框的"路径"文本框中输入 class 虚拟目录所对应的本地目录位置 C:\class。如果本地目录比较深，为了防止出现错误，可以单击"浏览"按钮，在弹出的对话框中选择正确的目录位置即可。

（4）单击"下一步"按钮，弹出如图 3-49 所示的对话框。在此对话框中，可以根据此目录的用处设置对此目录访问的权限，有效地保护目录中文件的安全性和正确性。

（5）单击"下一步"按钮，在弹出的对话框中，单击"完成"按钮，完成虚拟目录的设置。

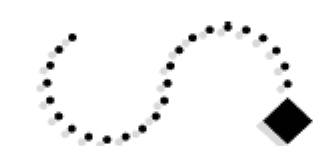




图 3-48　设置虚拟目录对应的实际目录位置

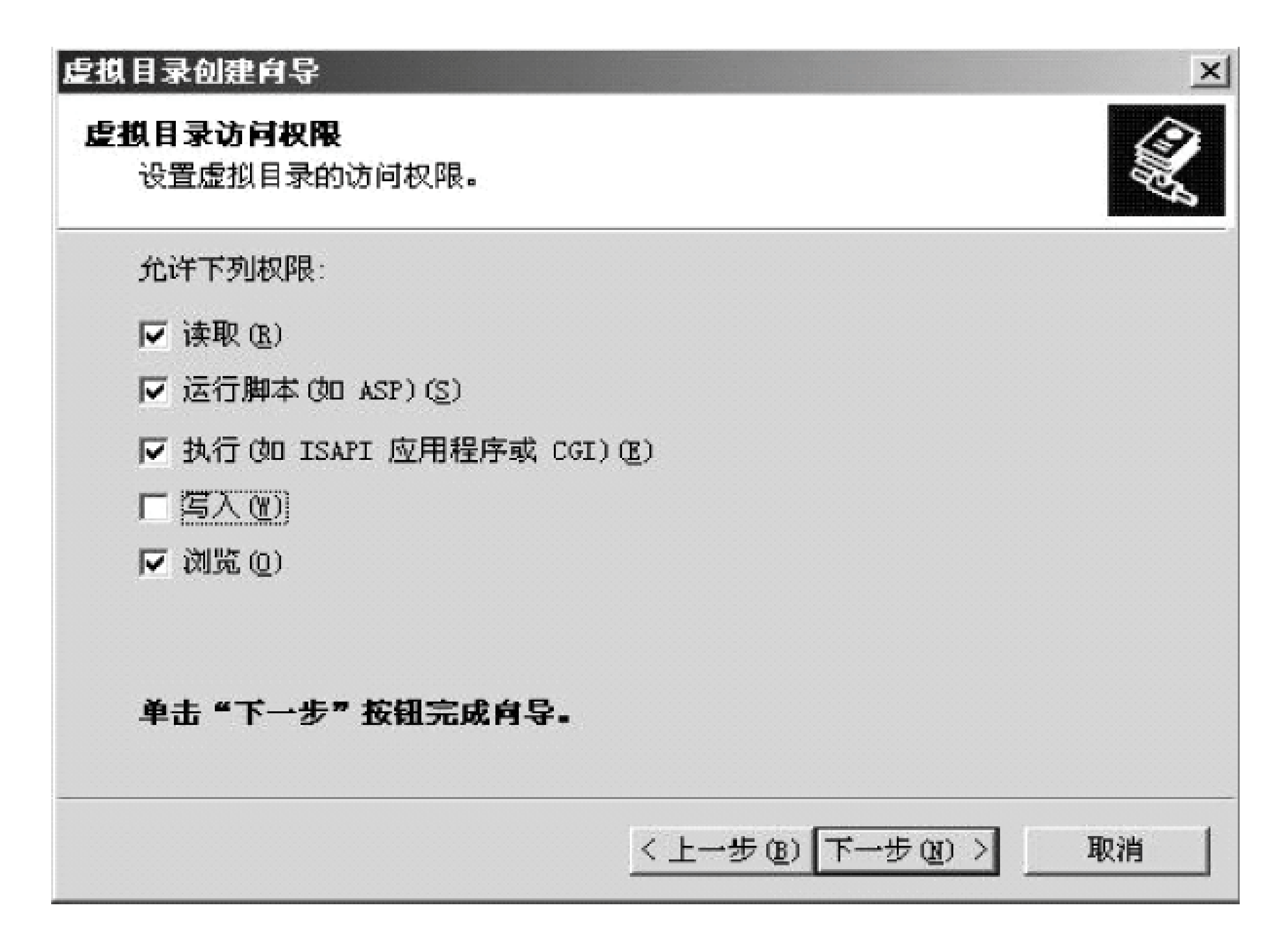


图 3-49　设置虚拟目录的访问权限

3. Web 服务器的管理

Web 管理器中还有很多设置，可以使用户对资源访问更加安全、稳定和便捷。这些设置主要通过 Web 站点属性对话框来实现。

(1)"网站"选项卡

在该选项卡中可以设置网站标识名称，配置对网站的访问权限，设置站点的连接限制，还可以启用日志记录并配置站点的日志记录格式，如图 3-50 所示。

① 在"描述"文本框中输入网站的标识名称。标识名称将出现在 IIS 管理器的控制台树中。

② 在"IP 地址"组合框中选择一个 IP 地址或输入用于访问该站点的新 IP 地址。如

图 3-50 “网站”选项卡

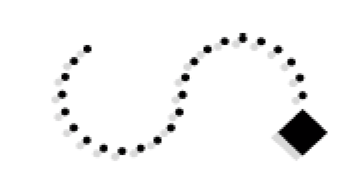
果没有分配指定的 IP 地址，那么此站点将响应分配给该计算机但没有分配给其他站点的所有 IP 地址，则该站点成为默认网站。

③ TCP 端口与 SSL 端口。在“TCP 端口”文本框中输入运行 Web 服务的 TCP 端口，默认的端口号是 80。可以将 TCP 端口更改成任何惟一的端口号，如果更改 TCP 端口号，必须预先通知客户端，以便客户端请求该更改的端口号，否则客户端的请求无法连接到服务器。TCP 端口号是必需的，该文本框不能为空。

在“SSL 端口”文本框中输入与该网站标识相关联的 SSL 端口号。默认的 SSL 端口号是 443。可以将 SSL 端口更改成任何惟一的 SSL 端口号，如果更改 SSL 端口号，必须预先通知客户端，以便客户端请求该更改的端口号。只有当站点使用 SSL 加密时才需要设置 SSL 端口号。如果没有为站点启用 SSL 加密，则“SSL 端口”文本框设置为空。

④ 在“连接超时”文本框中以秒为单位设置服务器断开不活动用户连接的时间长短，这将确保在 HTTP 协议无法关闭某个连接时，关闭所有的连接。大多数 Web 浏览器要求服务器在多个请求中保持连接打开，这需要选择“保持 HTTP 连接”复选框，它是可以极大增强服务器性能的 HTTP 规范。如果没有选择该复选框，浏览器将不得不为包含多个元素（如图形）的页面进行大量的连接请求，可能需要为每个元素进行单独连接。这些额外的请求和连接要求额外的服务器活动和资源，这将会降低服务器的效率。而其他请求特别是通过高滞后（慢）连接的请求，也可以使浏览器变慢并且响应变少。在安装过程中系统默认启用“保持 HTTP 连接”复选框。

⑤ 选择“启用日志记录”复选框可以启用网站的日志记录功能，记录关于用户活动的细节并按所选格式创建日志，日志记录的信息存储在 ASCII 文件或与 ODBC 兼容的数据库中。IIS 中的日志记录信息超出了 Microsoft® Windows® 事件日志或性能监视器功



能的范围。日志包括的信息诸如哪些用户访问了您的站点，访问者查看了什么内容，以及最后一次查看该信息的时间等。日志可以用来评估网站内容受欢迎程度或用来识别信息瓶颈。当需要进行日记记录时，用户要选择一种日志的格式。

“活动日志格式”下拉列表框中有 4 个选项。

- Microsoft IIS 日志文件格式是一种固定的 ASCII 格式。
- NCSA 共用日志文件格式是一种固定的 ASCII 格式。
- ODBC 日志记录是一种记录到数据库的固定格式，与该数据库兼容。
- W3C 扩展日志文件格式是一种可自定义的 ASCII 格式，该格式为系统的默认格式。要使用进程记账，必须选择 W3C 扩展日志文件格式。

(2)“主目录”选项卡

在此选项卡中可以在 IIS 服务器上创建和管理网站。此选项卡上的设置与虚拟目录的“主目录”选项卡上的那些可用设置相似。

(3)“文档”选项卡

在此选项卡中可以定义站点的默认网页并在站点文档中附加页脚。“文档”选项卡如图 3-51 所示。

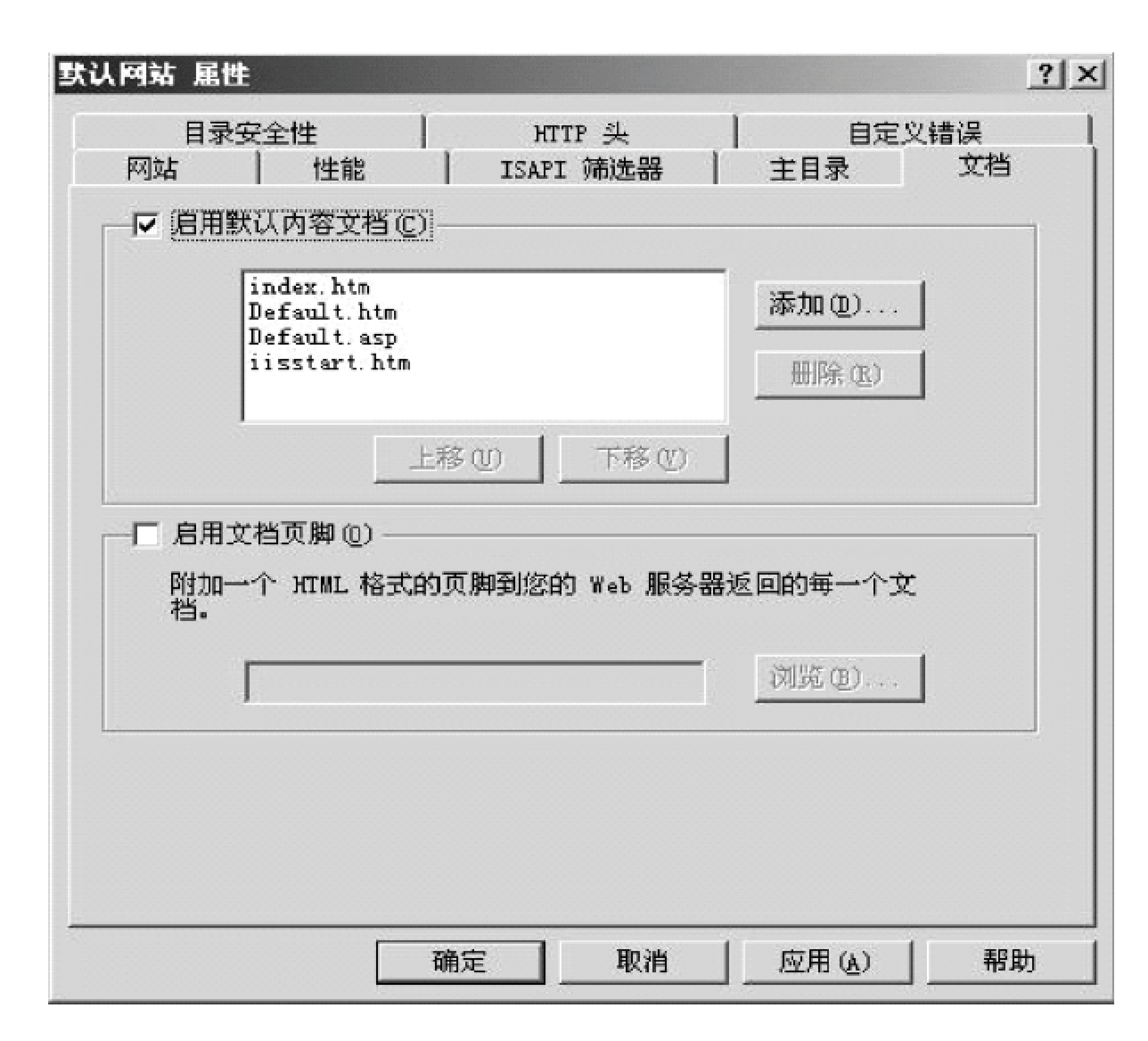


图 3-51　“文档”选项卡

① 选择“启用默认内容文档”复选框后，只要浏览器请求没有指定文档名称，则将默认文档提供给浏览器。默认文档可以是目录主页或包含站点文档目录列表的索引页。多个文档可以按照自上向下的搜索顺序列出。列表框中显示的文件可在站点的主目录中找到。单击“上移”和“下移”按钮可以调整文档的顺序。如果文档列表中只有一个文档，就可以自动地浏览其内容，如果有多个同时存在的文档，则按照先后顺序选择一个文档浏览。

② 选择“启用文档页脚”复选框，可以自动附加一个 HTML 格式的页脚到 Web 服务器返回的所有文档中。页脚文件不是完整的 HTML 文档，只包含格式化页脚内容的外观和功能及必要的 HTML 标记。

(4)“性能”选项卡

在该选项卡中可以设置网站的带宽限制以及客户端 Web 连接的数量。通过配置站点的网络带宽，可以更好地控制该站点允许的流量。例如，通过限制低优先级的网站上的带宽和(或)连接数，可以允许其他高优先级站点处理更多的流量负载。带宽限制和网站连接数量的设置是站点特定的，并可随着网络流量和使用情况的改变而进行调整。“性能”选项卡如图 3-52 所示。

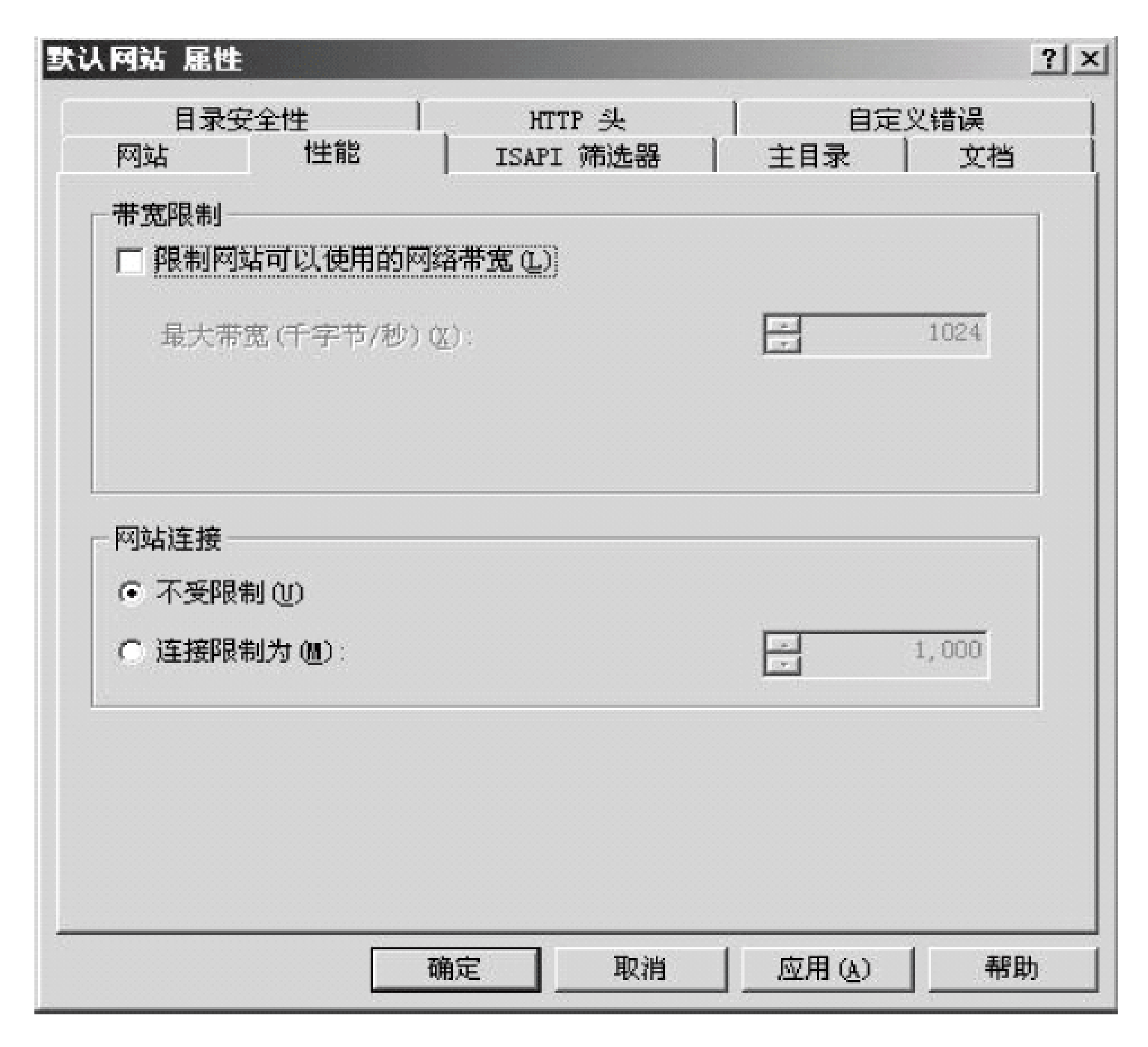


图 3-52 “性能”选项卡

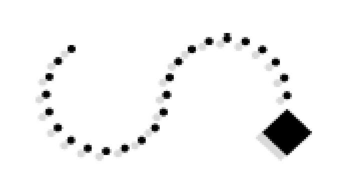
① 带宽限制。带宽限制限制了该网站可用的带宽。当发送数据包时，带宽限制使用数据包计划程序进行管理。当使用 IIS 管理器将站点配置成使用带宽限制时，系统将自动安装数据包计划程序，并且 IIS 自动将带宽限制设置成最小值 1024 千字节/秒。

选择“限制网站可以使用的网络带宽”复选框可以启用网站的带宽限制。

② 网站连接。用户可以将 Internet 信息服务(IIS)配置成允许数目不受限制的并发连接或限制该网站接收的连接个数。如果连接趋向于波动，则将连接数量设置成不受限制可以避免常量管理。但是，如果连接数超过了系统资源，则系统性能可能受到影响。将站点限定在特定的连接数可以保持系统性能的稳定。

(5)“HTTP 头”选项卡

在“HTTP 头”选项卡中，可以在 HTML 页的标题中设置返回到浏览器的值，也可以设置 HTML 页的内容分级以及定义 MIME 类型。可以对所有站点进行全局设置，也可以在每个站点中单独设置。Internet 信息服务(IIS)对这些设置使用继承模型。如果用



户更改了与层次结构中的其他节点处的设置有冲突的设置，那么系统将提示用户指定应用此新设置的节点。“HTTP 头”选项卡，如图 3-53 所示。

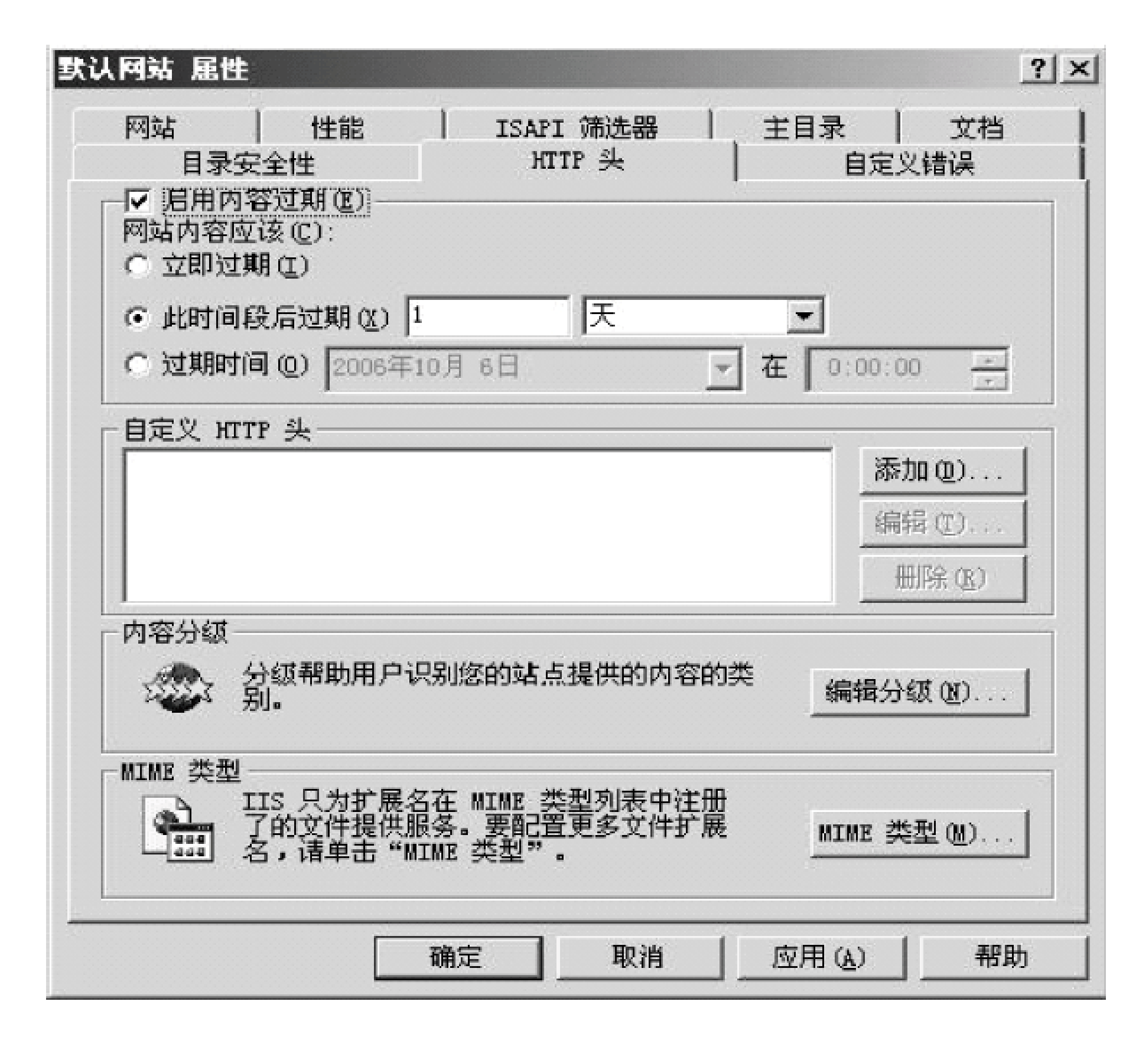


图 3-53　“HTTP 头”选项卡

① 启用内容过期。对于对时间敏感的材料（例如特定的报价或事件公告），应选择“启用内容过期”复选框，浏览器将当前日期与过期日期相比较来决定是显示一个缓存页，还是从服务器请求一个更新的页面。其中有 3 个单选按钮：

- 选中“立即过期”单选按钮后内容将立即过期。该设置强制浏览器总是从服务器上检索有关后续请求的最新内容。
- 选中“此时间段后过期”单选按钮后可以设置特定的时间段，超过该时间段后则强制浏览器重新从服务器上检索有关后续请求的内容。
- 选中“过期时间”单选按钮后可以设置特定的日期和时间，超过该日期和时间后则强制浏览器重新从服务器上检索有关后续请求的内容。

② 自定义 HTTP 头。可以使用该属性自定义 HTTP 头从 Web 服务器发送到客户端浏览器。自定义 HTTP 头可用来将当前 HTTP 规范中尚不支持的指令从 Web 服务器发送到客户端，例如，产品发布时 IIS 尚不支持的更新的 HTTP 头。

4. Web 站点的测试

配置 Web 站点后，还需要进行 Web 站点的测试。

将用户做好的 Web 页面放置到我们设置的 Web 站点的根目录中，即 D:\myserver.net\www 目录中。启动 IE 浏览器，在地址栏中输入网址，例如，http://localhost[/网页文件名]或 http://＜本机域名＞[/网页文件名]，按回车键。注意：地址栏中如果输入了一个域名，则相应的 DNS 应该配置正确，能够正确地解析域名对应的主机 IP 地址。如果屏幕显示的内容是用户刚做好的网页，则证明站点的配置是正确的。如果屏幕上有提示

 性信息，应根据信息的内容再进行调试。Web 站点的测试结果如图 3-54 所示。



图 3-54　Web 站点的测试

3.3.3　FTP 站点的建立与管理

文件传输协议 FTP(File Transfer Protocol)是 Internet 上使用最为广泛的文件传送协议。FTP 提供交互式的访问，允许用户指名文件的类型与格式，并允许文件具有存取权限。FTP 系统是一个通过 Internet 传输文件的系统，它支持文本文件、图形图像文件以及声音文件和程序文件等的传输。用户从 FTP 服务器上把所需文件或资源传送到自己的计算机上的过程称为 FTP 的下载；用户将文件从自己的计算机上发送到 FTP 服务器上的过程称为 FTP 的上传。

FTP 采用客户机/服务器模式进行工作，所以客户机必须建立与远程 FTP 服务器的连接，并且登录后才能进行文件传输。通常情况下，登录 FTP 服务器的方式有两种。

- 匿名登录。采用这种方式，用户可以免费访问 FTP 服务器，并且可索取文件，匿名登录不要求用户事先在该服务器进行注册，服务器就能够无偿提供对文件的复制服务。匿名登录方式的用户名为 anonymous，密码为任意符号或空。
- 实名登录。实名登录要求用户在登录 FTP 服务器之前，必须先向该服务器的系统管理员申请用户名及密码，该方式主要用于 FTP 服务器内部或外部的有偿信息服务。采用这种方式登录时，系统要求提交真实存在的用户名及密码，并进行身份认证。实名登录可以有效地保护私人用户的数据安全及个人隐私。

1. 建立 2003server. myserver. net FTP 服务器

有一个服务器，域名为 2003server. myserver. net，IP 地址为 192. 168. 1. 10，在其上配置当前域的 FTP 服务，其 FTP 服务文件存放的主目录位于 D:\myserver. net\ftp，并且可以进行上传和下载。其设置步骤如下：

(1) 在“Internet 信息服务(IIS)管理器”窗口中，右击“FTP 站点”中的“默认 FTP 站点”，在弹出的快捷菜单中选择“属性”命令，如图 3-55 所示。

(2) 在弹出的“默认 FTP 站点属性”对话框中，根据需要进行 IP 地址和 TCP 端口号及超时时间、账户安全设置、主目录位置和目录安全性的设置。

(3) IP 地址和端口的设置。在“IP 地址”组合框中指定一个 IP 地址或输入用于访问该站点的新 IP 地址。如果没有分配指定的 IP 地址，那么此站点将响应分配给该计算机但没有分配给其他站点的所有 IP 地址，使它成为默认网站。要使 IP 地址出现在列表中，必须在“控制面板”窗口中定义了此 IP 地址可在该计算机上使用。

FTP 服务运行的 TCP 端口的默认端口号是 21。可以在“TCP 端口”文本框中将端口号更改为任何惟一的 TCP 端口号，但是客户端必须事先知道才能请求该端口号，否则其请求不能连接到服务器。TCP 端口号是必需的，该文本框不能为空。

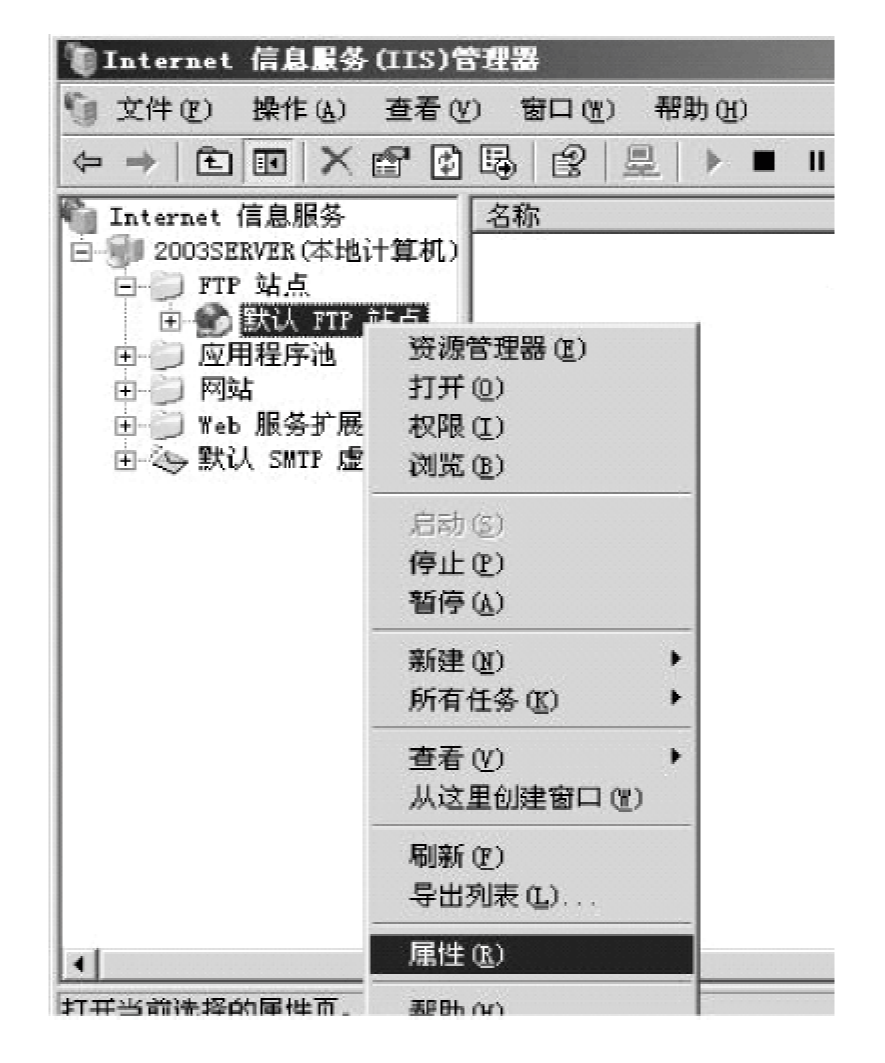


图 3-55　FTP 站点的创建



图 3-56　FTP 站点 IP 地址和 TCP 端口设置

根据题目，这里使用默认的配置即可，如图 3-56 所示。

(4) 安全账户登录设置。在“安全账户”选项卡中可以管理该 FTP 站点的账户。用户可以指定用于匿名客户端请求登录到计算机的账户，并且可以控制具有站点操作员权限的那些用户。如果使用匿名登录，则将“允许匿名连接”复选框选中，在“用户名”和“密码”文本框中输入一个本地主机的一个账号。如果选中“只允许匿名连接”复选框，则用户就不能使用用户名和密码登录。此选项可避免具有管理权限的账号访问，而只允许以匿名账号登录。

根据题目，选择“允许匿名连接”复选框但不选择“只允许匿名连接”复选框，如图 3-57 所示。

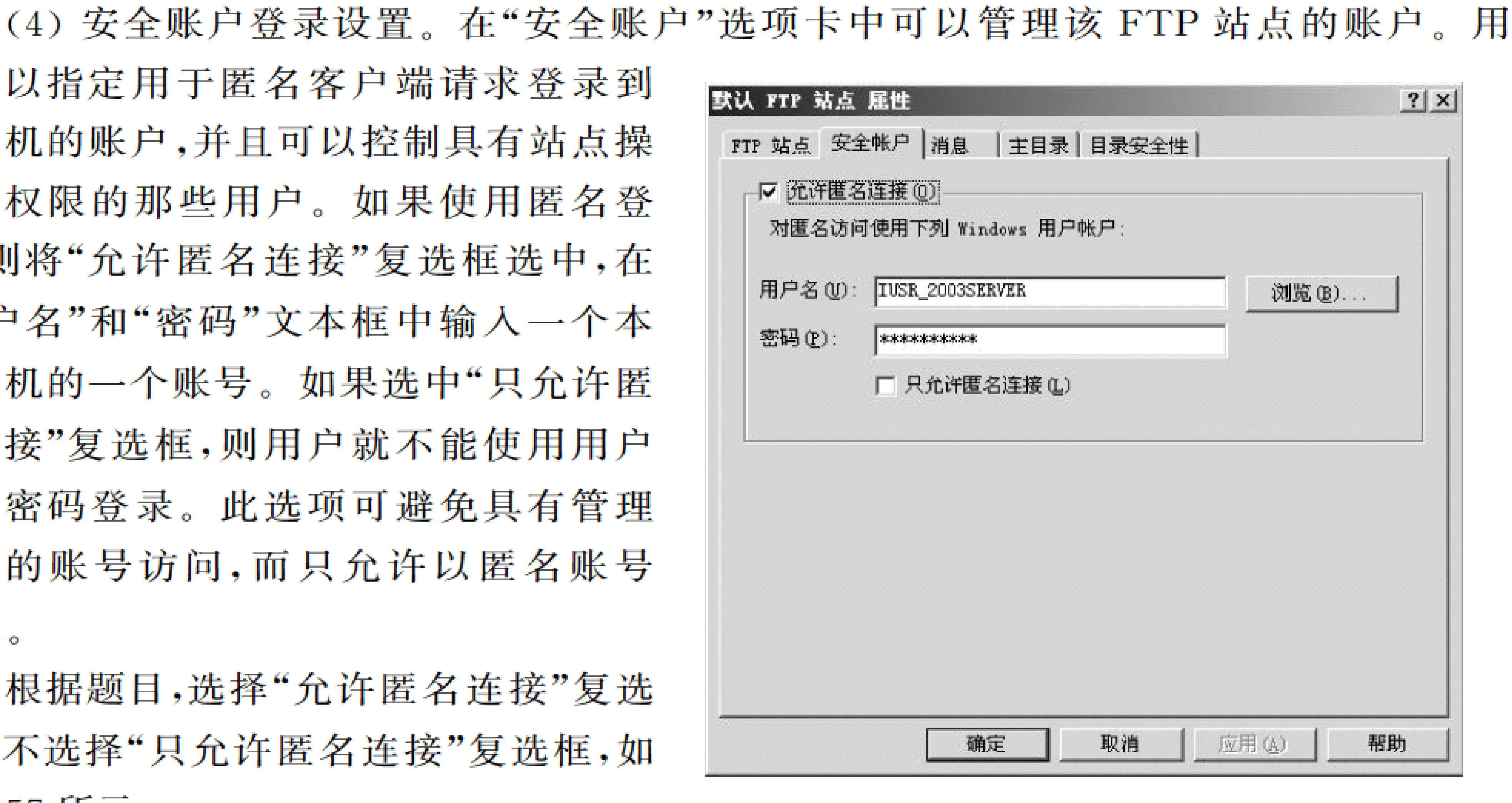
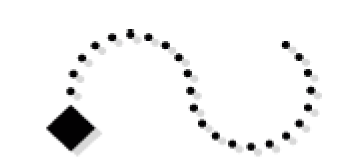


图 3-57　安全账户设置



（5）主目录位置及访问权限设置。在“主目录”选项卡中可以更改 FTP 站点的主目录或修改其属性。主目录是 FTP 站点中用于存储已发布文件的目录。在安装 FTP 服务时，系统将创建存储在 %localdrive%\inetpub\ftproot 中的默认主目录。

对于 FTP 主目录位置的设置，有两个单选按钮可供选择：

- 选择“此计算机上的目录”单选按钮，指定的目录是本计算机上的某一个目录；
- 选择“另一台计算机上的目录”，利用网络进行文件目录访问。在此文本框中输入服务器名和目录名。文件和目录在其他计算机上存储。

为了更好地对目录进行访问，可以对目录进行权限上的设置。权限包括 3 种：

- 读取：设置该权限允许用户读取或下载存储在主目录或虚拟目录中的文件。
- 写入：设置该权限允许用户向服务器中已启用的目录上传文件。应该仅对要接收用户文件的目录启用写入权限。
- 记录访问：设置该权限将对该目录的访问记录到日志文件中。只有为该 FTP 站点启用日志记录时才记录访问。默认情况下启用日志记录。

根据题目要求，在“此资源的内容来源”选项组中选择“此计算机上的目录”单选按钮，在“本地路径”文本框输入 FTP 站点目录为 D:\myserver.net\ftp，设置用户对此目录文件的访问权为完全控制，即选择“读取”、“写入”、“记录访问”3 个复选框，如图 3-58 所示。

（6）目录安全性设置。在“目录安全性”选项卡中可允许或阻止单个计算机或计算机组访问 FTP 站点。通过将计算机的 TCP 或 IP 地址指定为授权或拒绝访问权限，可以控制对 FTP 资源的访问，例如站点、虚拟目录或文件。在“下面列出的除外”列表框中输入授权或拒绝之外的主机。如果没有特例，则所有访问的主机按照授权或拒绝进行对资源的访问，如图 3-59 所示。

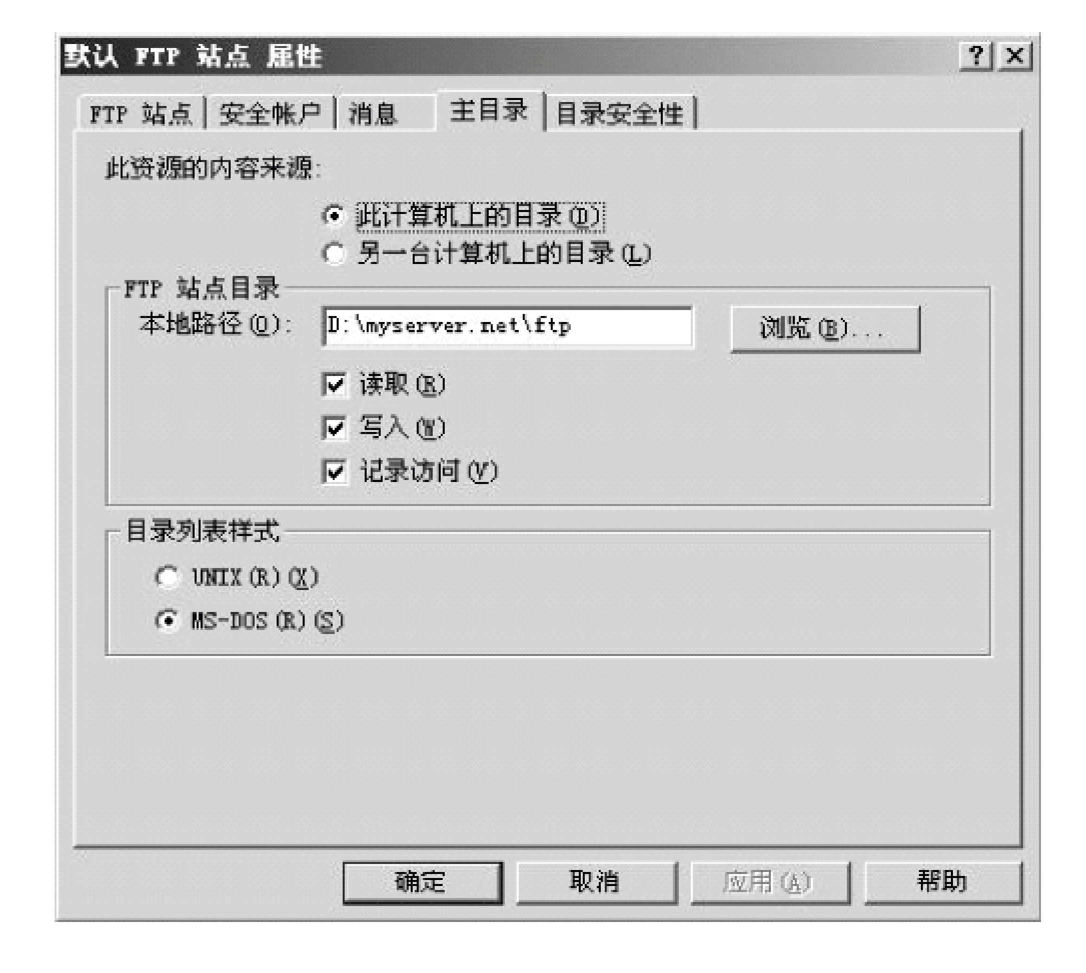



图 3-58　FTP 主目录设置

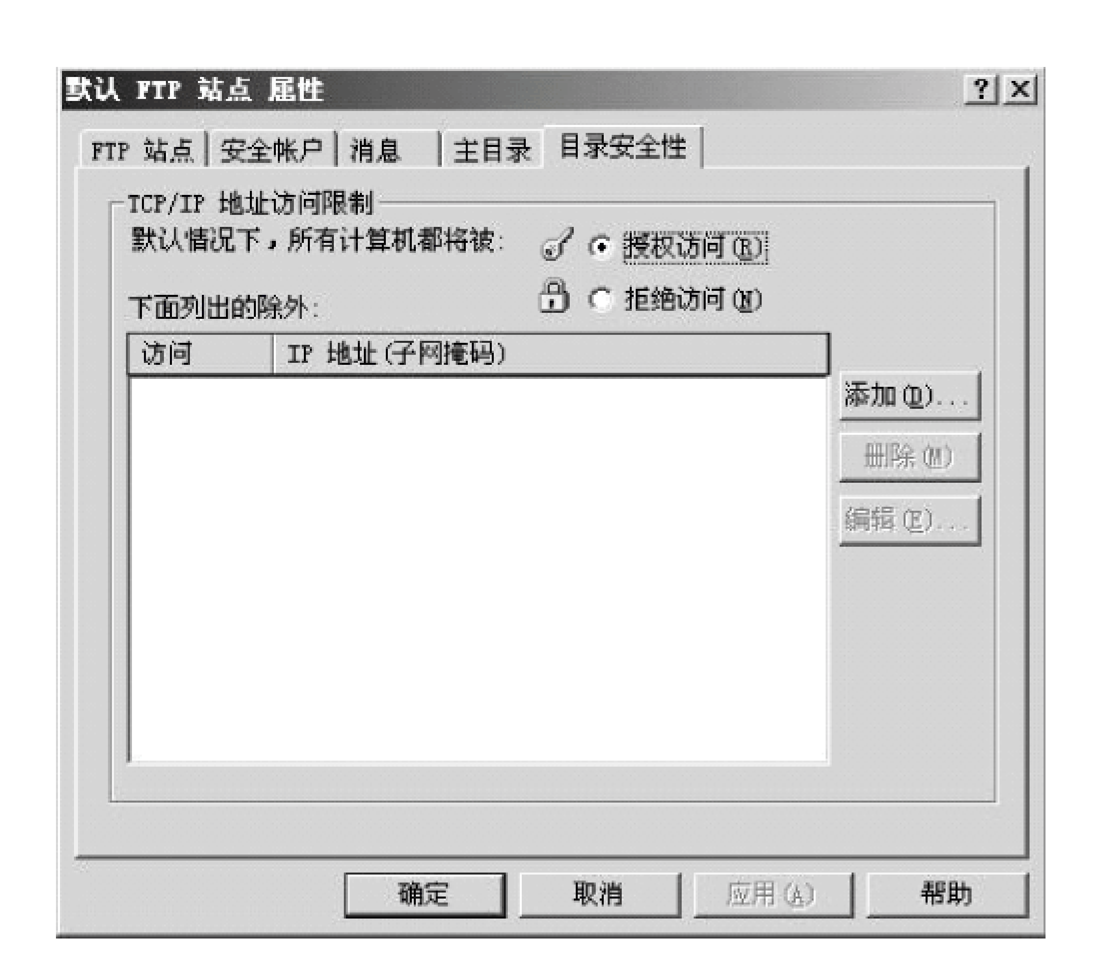
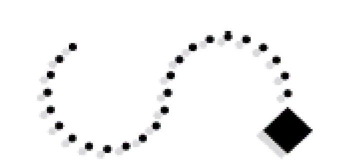


图 3-59　FTP 的目录安全性设置

根据题目要求，选中“授权访问”单选按钮，且不设置任何例外。

（7）所有设置完毕，单击“确定”按钮，完成 FTP 站点的属性设置。

至此，一个基于本地目录的 FTP 服务器设置完毕。为了保证 FTP 设置的有效性，还



要对设置的服务器进行测试。

2. 测试 FTP 站点

FTP 站点的测试与 Web 站点的测试相似。

首先，将一些文件或目录复制到 FTP 站点的虚拟根中。然后，打开 IE 浏览器，在地址栏中输入 FTP 站点的地址，如 ftp://localhost 或 ftp://<本机 IP>，按回车键。如果测试显示的文件和目录与复制的一样，并且能够以匿名或非匿名方式进行登录，则表示 FTP 站点设置正确。

3.4　综合实训

假设某单位的域名为 sjsyd.com.cn，其单位有相关服务器，请根据下面的要求进行相关配置。

(1) 配置 DNS 服务。此单位域名服务器的地址为 172.16.32.4，此域下域名及 IP 地址的对应关系，如表 3-1 所示。请配置 DNS 服务，使其可以使用域名访问某个主机。

表 3-1　域名和 IP 地址对应表

域　　名	IP 地址	域　　名	IP 地址
www.sjsyd.com	172.16.32.2	dhcp.sjsyd.com	172.16.32.5
ftp. sjsyd.com	172.16.32.3	mail.sjsyd.com	172.16.32.6
dns.sjsyd.com	172.16.32.4	sql.sjsyd.com	172.16.32.7

(2) 配置动态 IP 地址分配服务(DHCP)。在此域下，有一网络区域经常有一些笔记本设备加入到当前区域中，所以要给予其本区域可用的 IP 地址。请设置一 DHCP 服务器，可用地址范围为 172.16.32.100～172.16.32.200，掩码为 255.255.255.0。此域的 DNS 地址为 172.16.32.4，网关为 172.16.32.1。每个 IP 地址的有效期为 1 天。

(3) 配置 Web 服务。配置 www.sjsyd.com.cn 主机，其下有一虚拟目录，名为 home，其对应的主目录为本地目录 C:\www，设置对此目录的访问权为只读，并将 C:\www\index.html 设置为默认文档。

(4) 配置 FTP 服务器。设置 FTP 服务器，使域中所有主机都可以利用 FTP 服务，共享资源。FTP 的 URL 地址为 ftp://ftp.sjsyd.com.cn/sharefiles。要求 FTP 服务器对 sharefiles 目录开放所有权限，让每一个用户都能进行资源的读写，并且 FTP 服务器支持匿名登录和实名登录。

要配置这一章的实训，首先要进行分析，分析需要几个服务器进行网络服务管理，然后就是对软件服务进行安装。在服务器上安装相应的 DNS、DHCP、IIS、FTP 等服务器的支持软件接口。在“控制面板”→“添加或删除程序”→“添加/删除 Windows 组件”窗口中可以找到相应的服务，并进行安装，如图 3-60 所示。最后进行服务器升级，利用 dcpromo 命令将工作站升级为域控制器，域名为 sjsyd.com.cn。以上是进行此次实训的前提条件，接下来就可以配置其中的服务了。

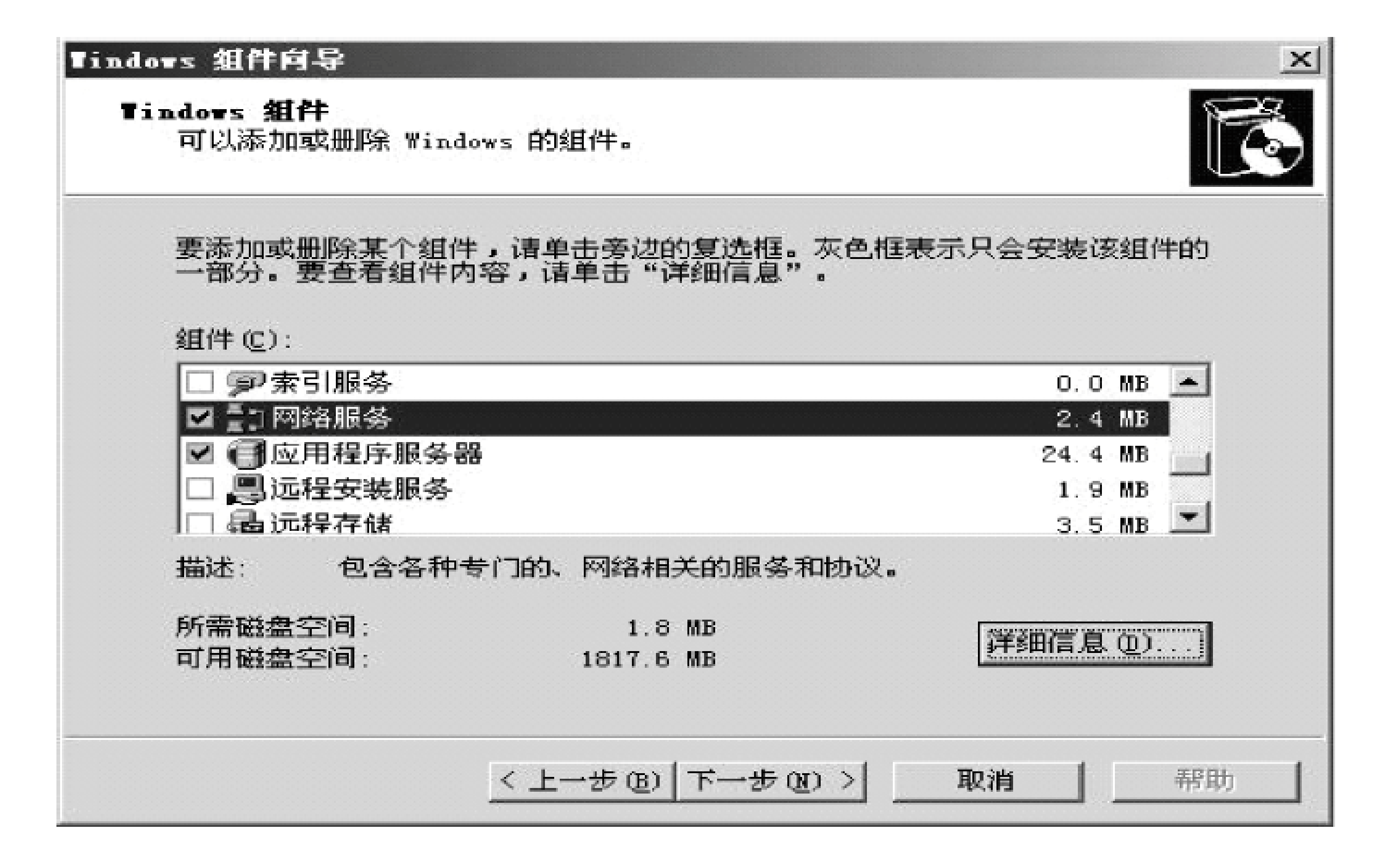


图 3-60　添加/删除 Windows 组件

1. DNS 配置

操作步骤如下：

（1）选择"开始"→"程序"→"管理工具"→DNS 命令，在弹出的窗口中右击服务器名称，在弹出的快捷菜单中选择"新建区域"命令，如图 3-61 所示。

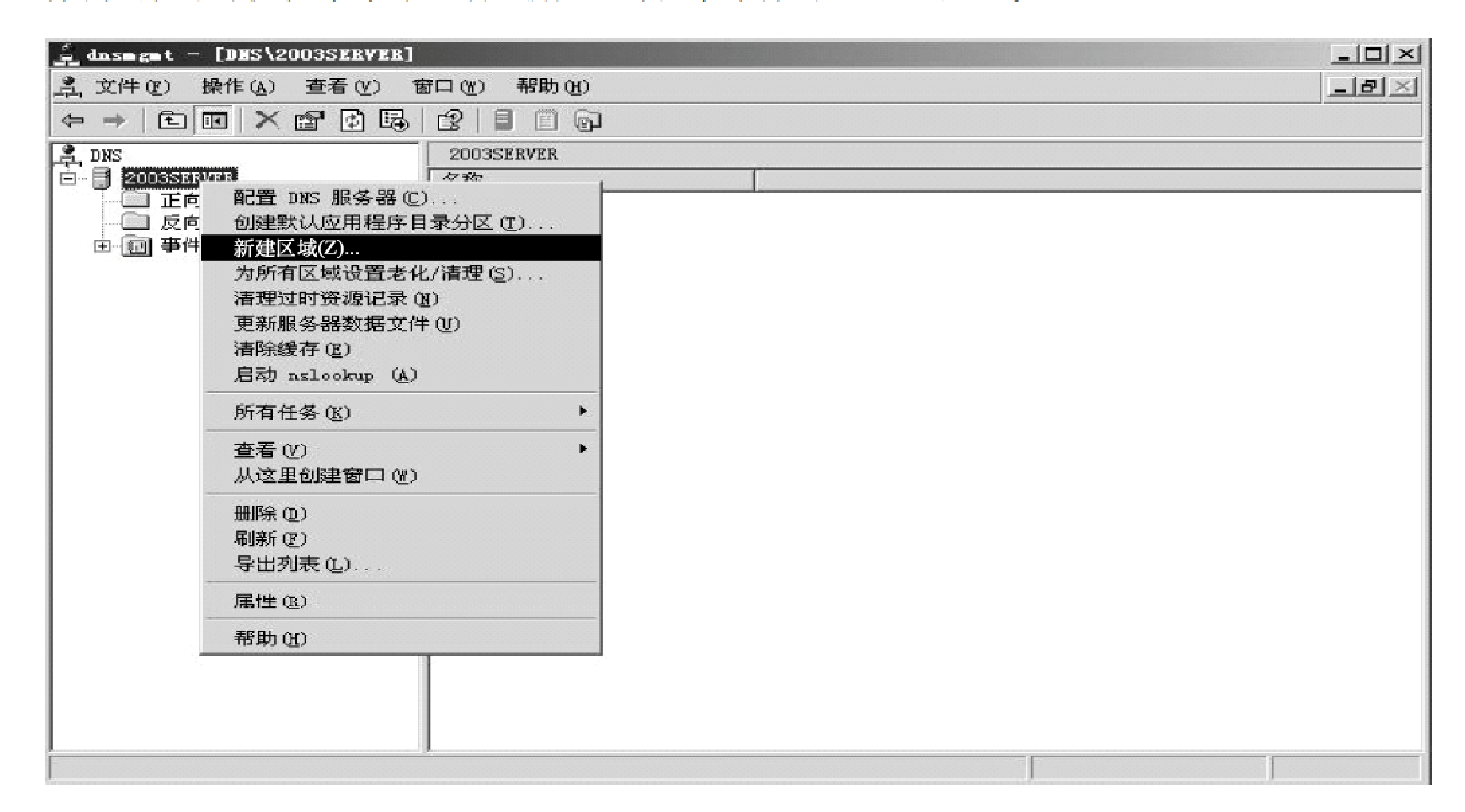
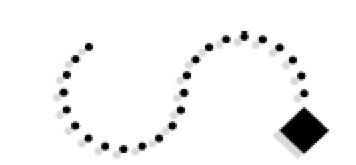


图 3-61　配置 DNS 区域

（2）按照弹出的"新建区域向导"对话框中的步骤创建主区域中的正向查找区域，区域名称为 sjsyd. com. cn，如图 3-62 所示。根据向导提示说明单击"下一步"按钮，最终完成正向查找区域的建立。



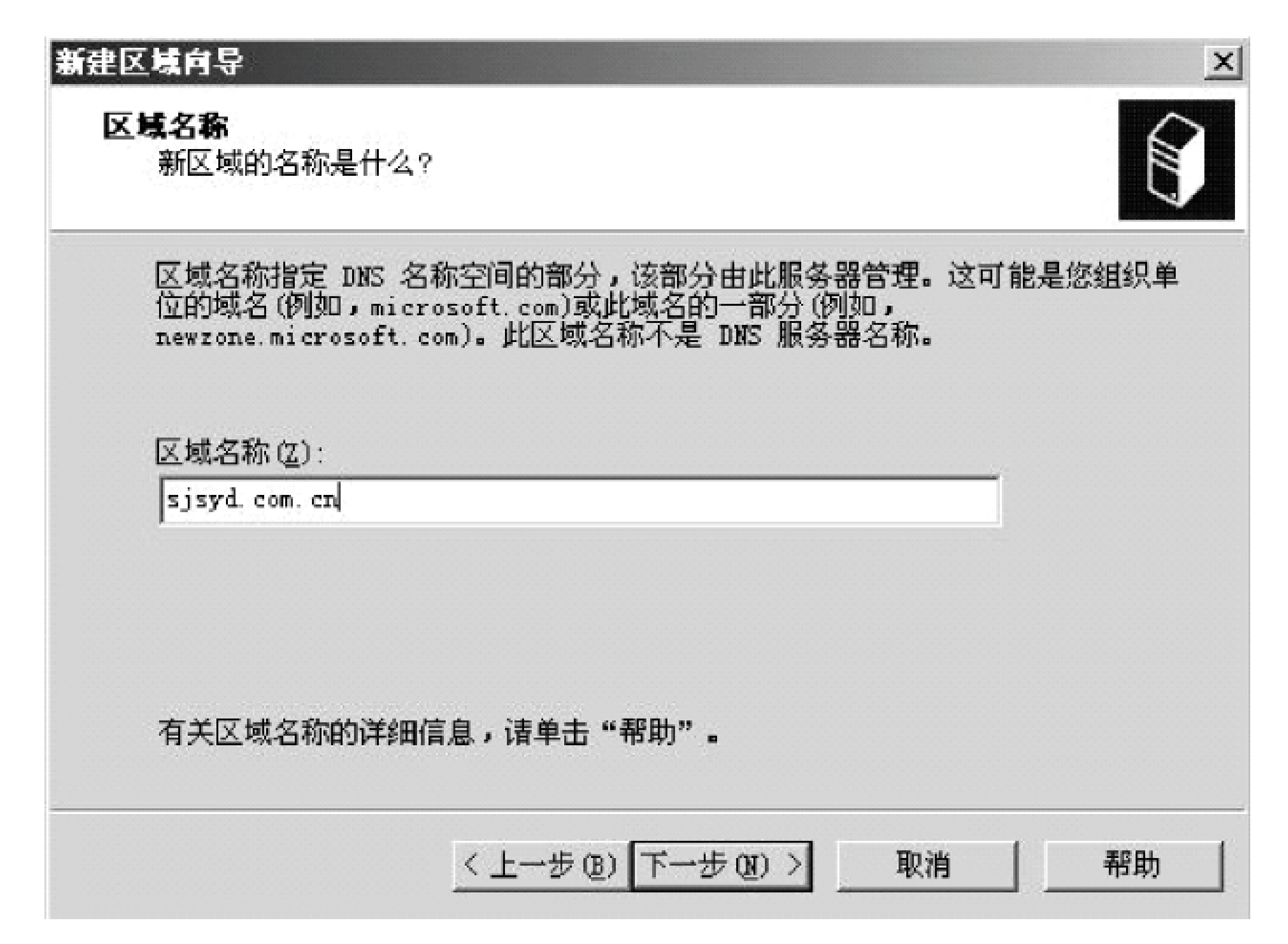


图 3-62　建立正向查找区域

(3) 按照建立正向域的方法建立反向查找区域，区域的 IP 地址段为 172.16.32.0/24，如图 3-63 所示。根据提示信息最终完成反向查找区域的建立。所有区域建立完成，如图 3-64 所示。

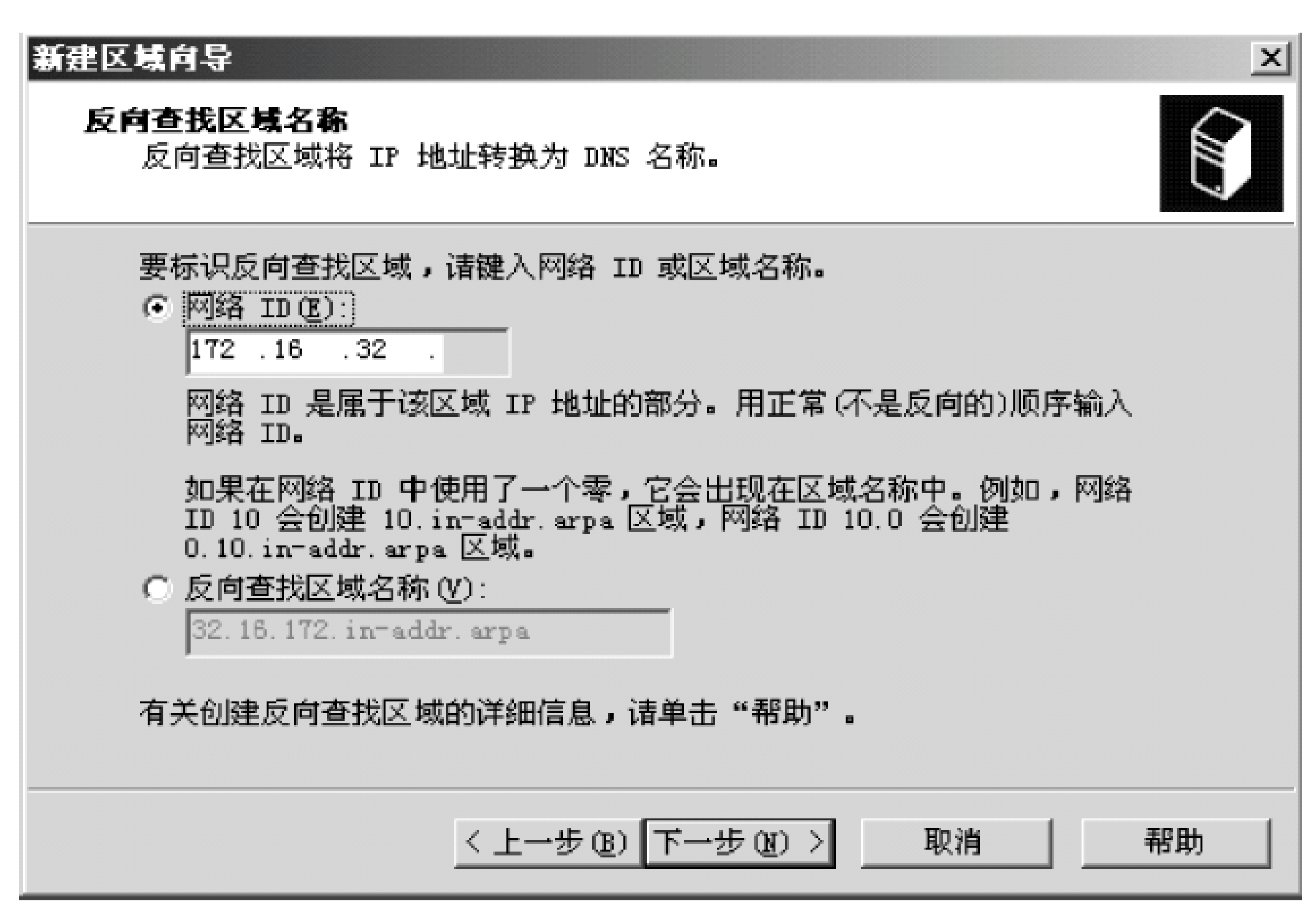


图 3-63　建立反向查找区域

(4) 建立好区域后，可以向区域中添加相应的记录，实现域名的解析。右击正向查找区域 sjsyd.com.cn，在弹出的快捷菜单中选择“新建主机”命令，如图 3-65 所示。

(5) 在弹出的“新建主机”对话框中输入相应的 IP 地址和域名，如图 3-66 所示。选择“创建相关的指针(PTR)记录”复选框可以省略向反向查找区域中添加记录的过程，单击“添加主机”按钮，系统会自动向反向查找区域中添加主机记录，实现双向的解析。

(6) 按照这种方法，将所有的记录添加到 DNS 服务器的记录集里，记录添加好之后就可以进行 IP 地址和域名之间的解析服务了。正向解析域如图 3-67 所示，反向解析域如图 3-68 所示。

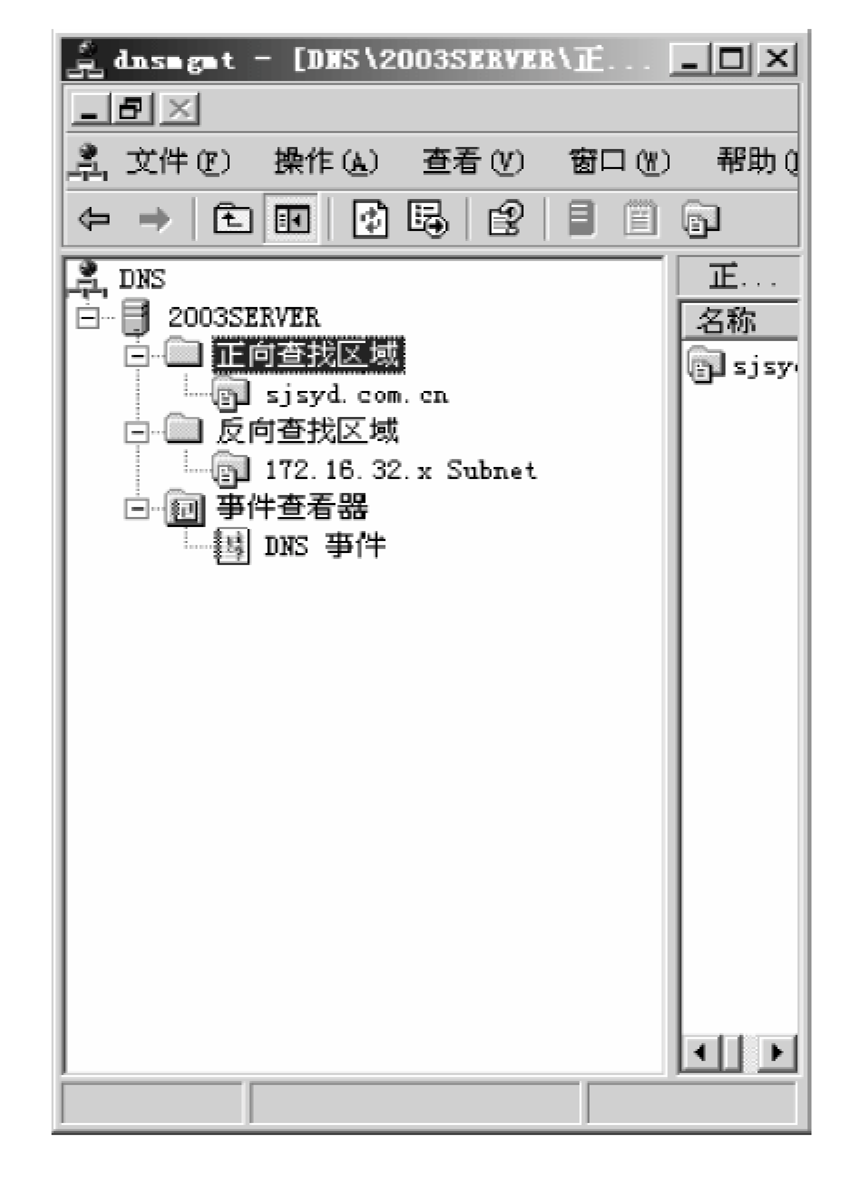


图 3-64 DNS 正向和反向查找区域

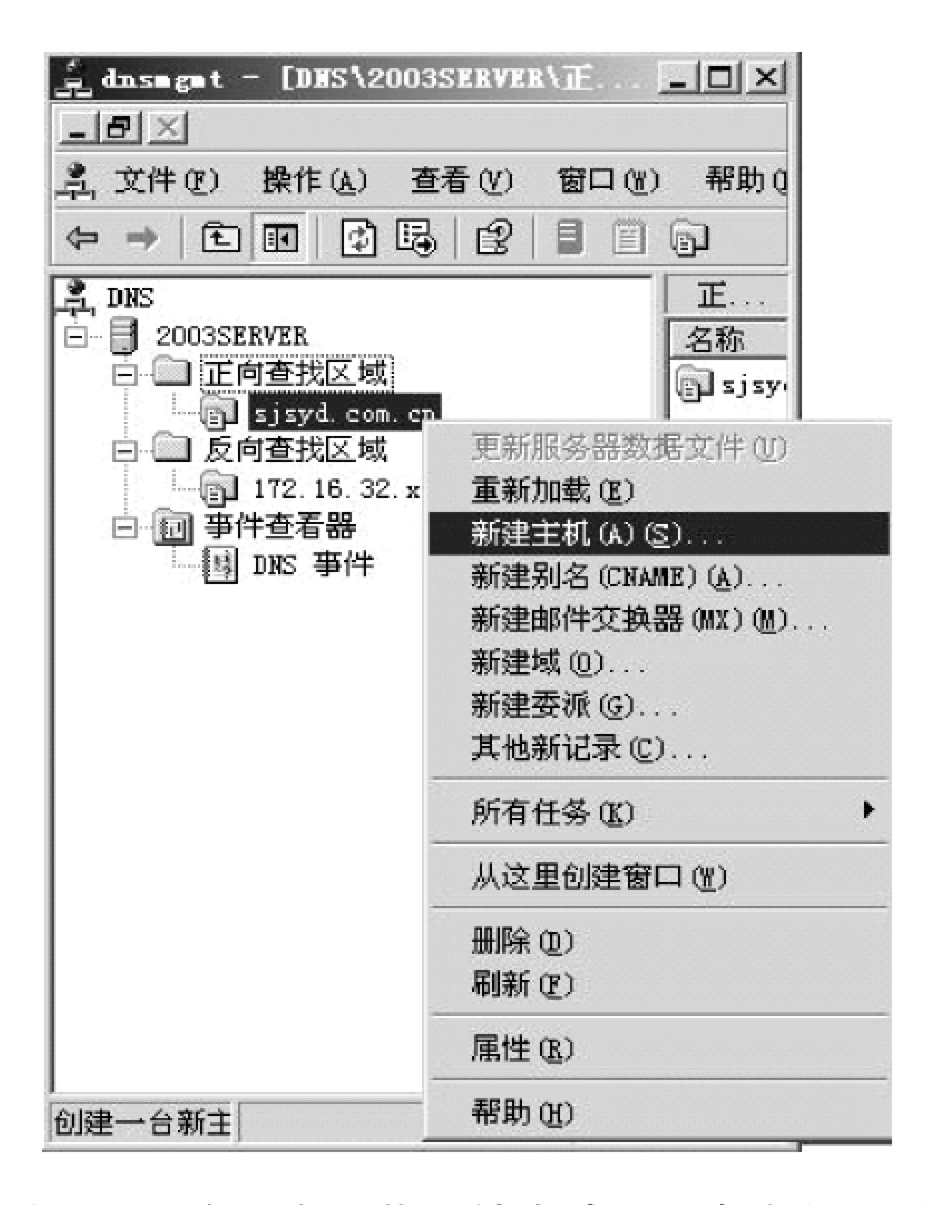


图 3-65 在正向查找区域中建立一条主机记录

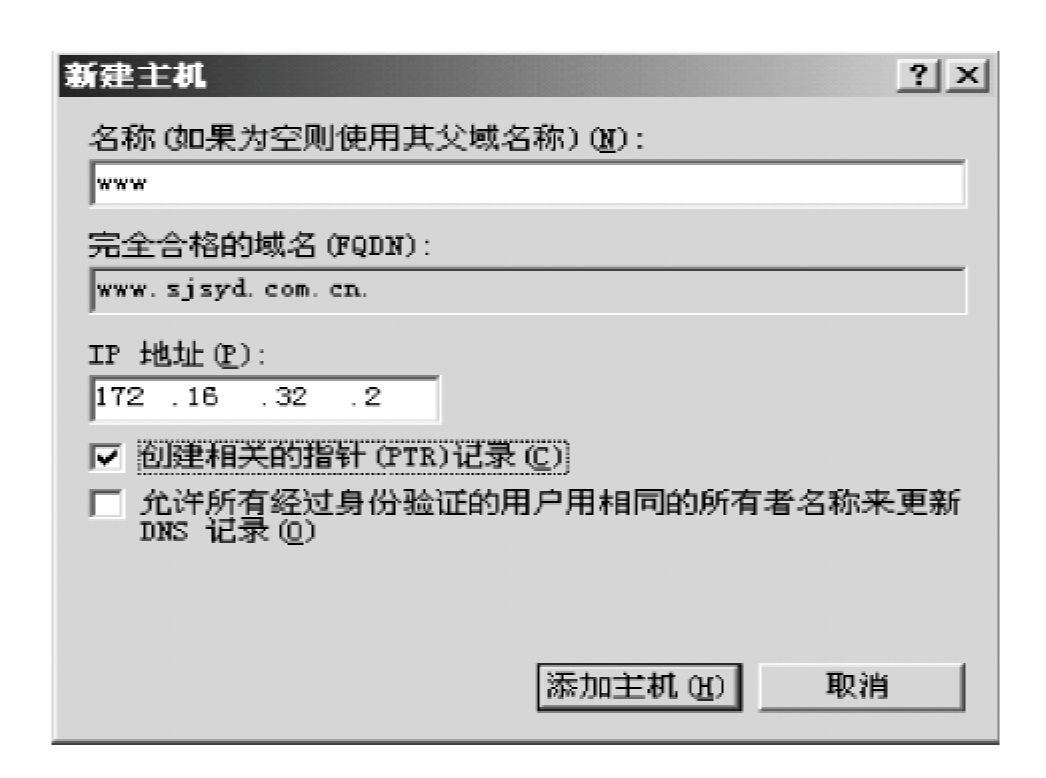


图 3-66 向 DNS 中输入相应的域名及 IP 地址

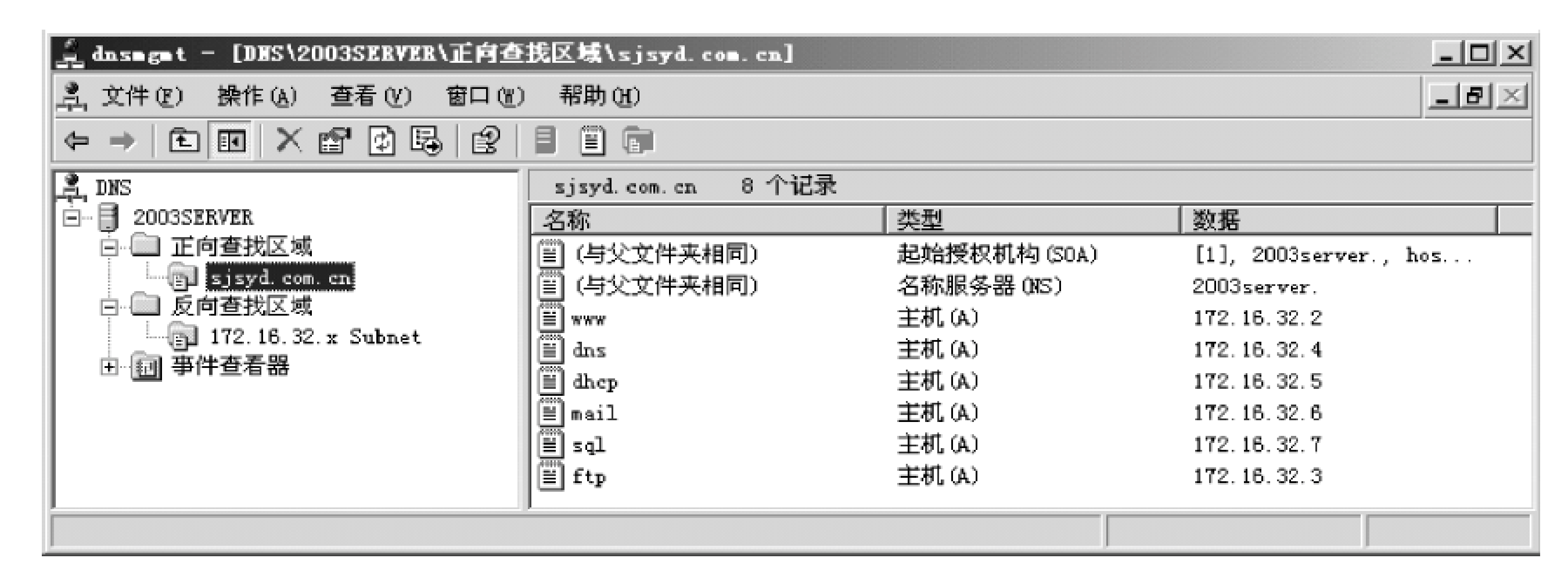
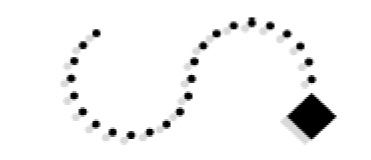


图 3-67 正向解析域



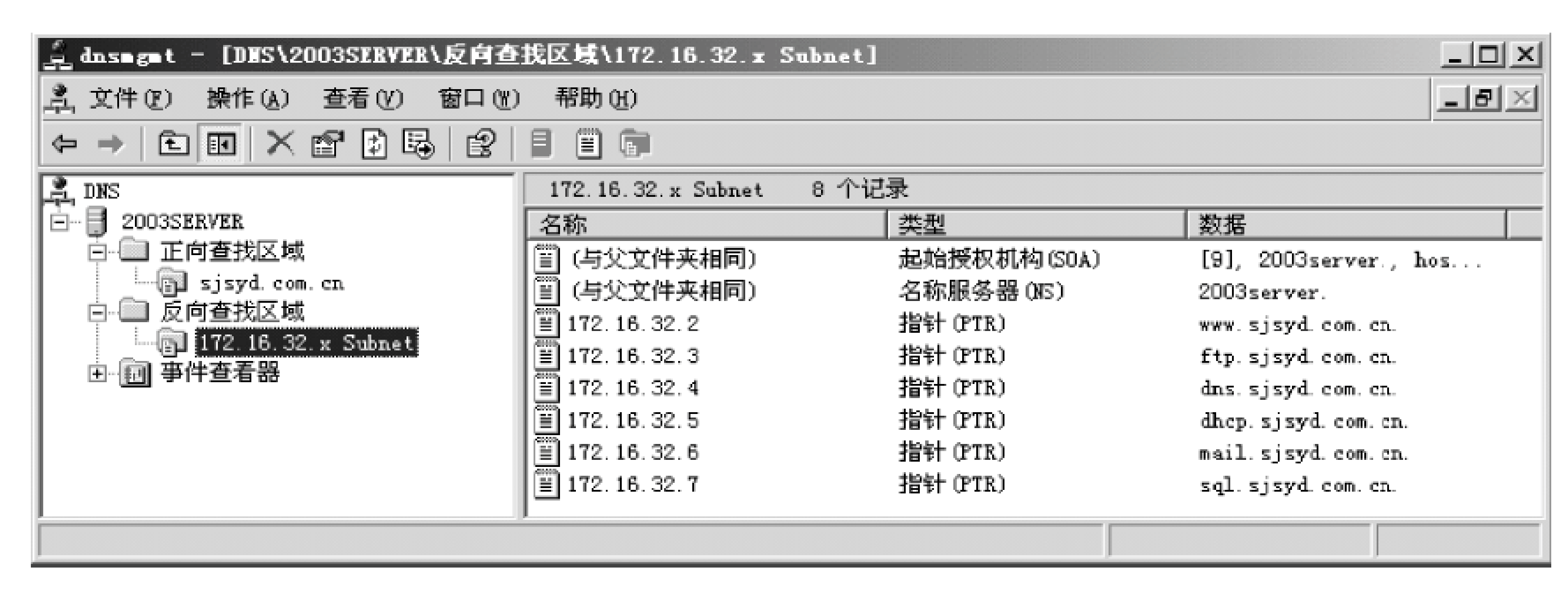


图 3-68　反向解析域

2. DHCP 服务设置

操作步骤如下：

(1) 首先启动 DHCP 服务器，在相应的服务器名称上右击，在弹出的快捷菜单中选择“授权”命令，然后在快捷菜单上选择“新建作用域”命令，如图 3-69 所示。

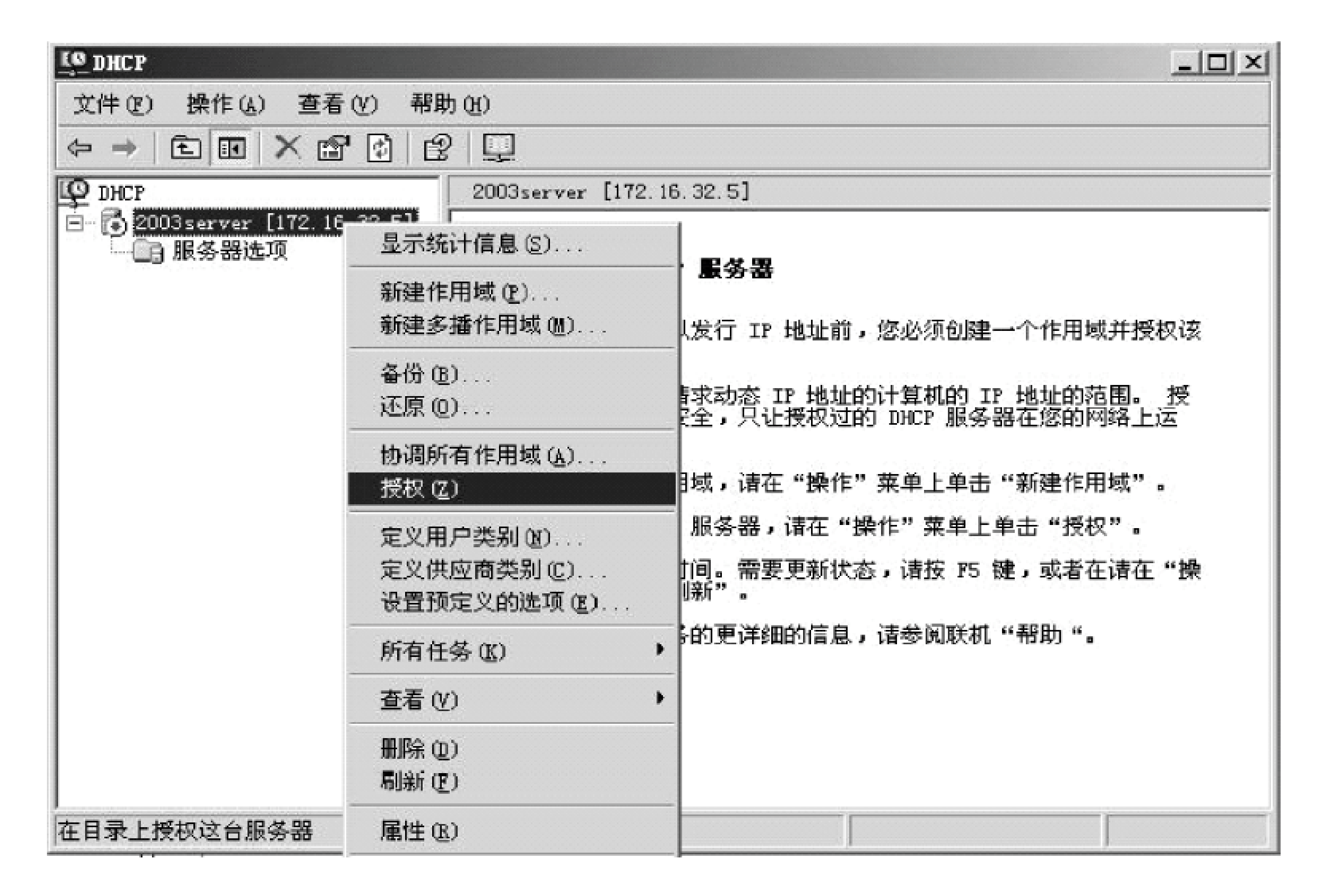


图 3-69　授权 DHCP 服务器

(2) 在弹出的对话框中，输入作用域名称 sjsyd.com.cn，如图 3-70 所示。

(3) 单击“下一步”按钮，在弹出的对话框中为创建的动态分配域输入可用的 IP 地址范围和此域的子网掩码长度，如图 3-71 所示。

(4) 单击“下一步”按钮，由于没有任何的其他 IP 地址在这个范围内，所以“排除的地址范围”列表框不需要填写。

(5) 单击“下一步”按钮，在弹出的对话框中设置动态分配的 IP 地址使用的租期为 1 天，如图 3-72 所示。

新建作用域向导

作用域名
您必须提供一个用于识别的作用域名称。您还可以提供一个描述(可选)。

为此作用域输入名称和描述。此信息帮助您快速标识此作用域在网络上的作用。

名称(A): sjsyd.com.cn
描述(D):

< 上一步(B)　下一步(N) >　取消

图 3-70　输入 DHCP 服务的域名称

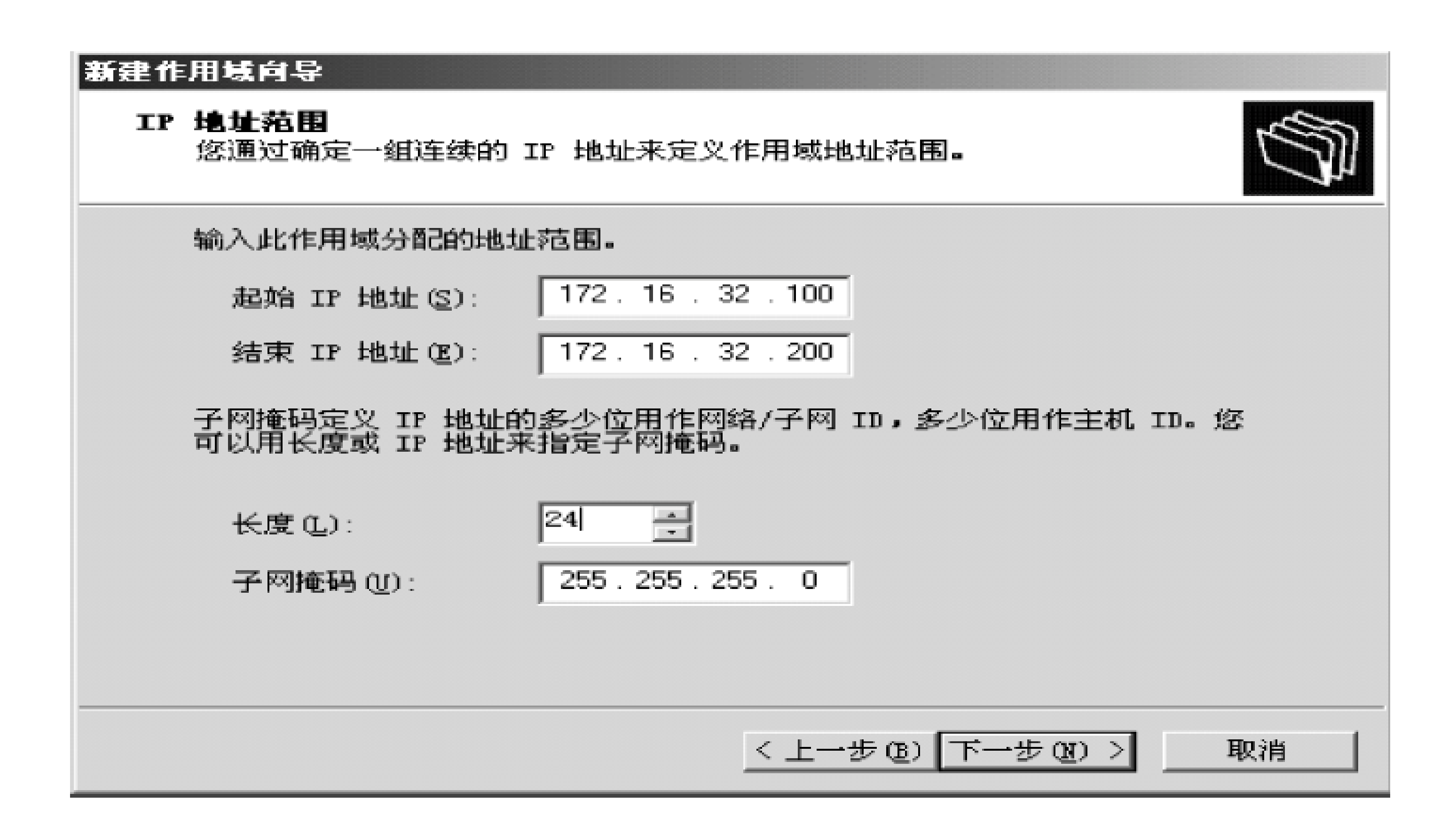


图 3-71　输入 DHCP 的起始和终止的 IP 地址

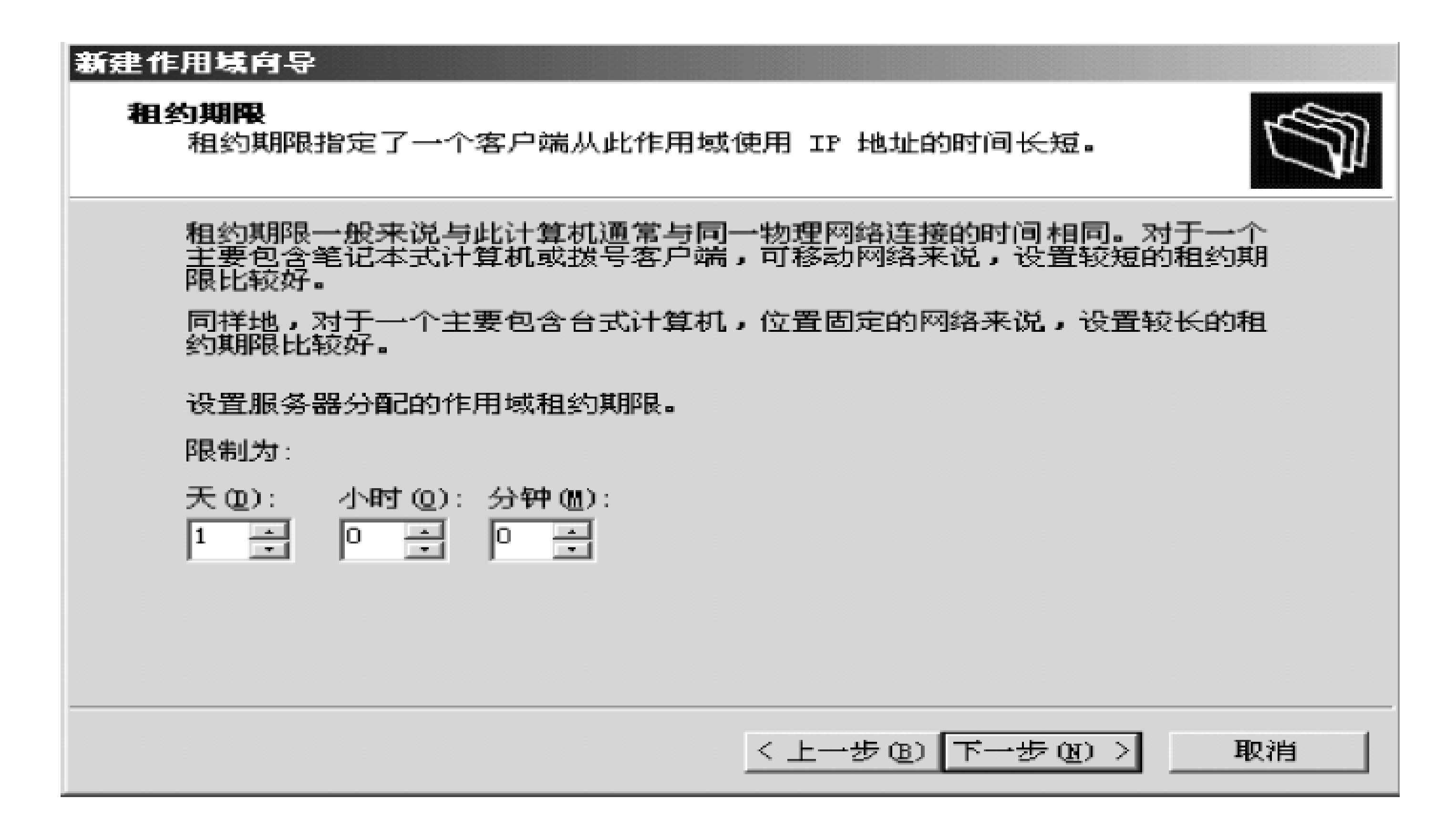


图 3-72　设置 DHCP 服务的 IP 地址租期

（6）单击“下一步”按钮，在弹出的对话框中选择“是，我想现在配置这些选项”单选按钮。

（7）单击“下一步”按钮，在弹出的对话框中设置 DHCP 其他选项，如 DNS 地址、网关路由地址等。

（8）最后，在“激活作用域”向导中选择“激活”，最终单击“完成”按钮即可配置好一台 DHCP 动态 IP 地址分配服务器，如图 3-73 所示。

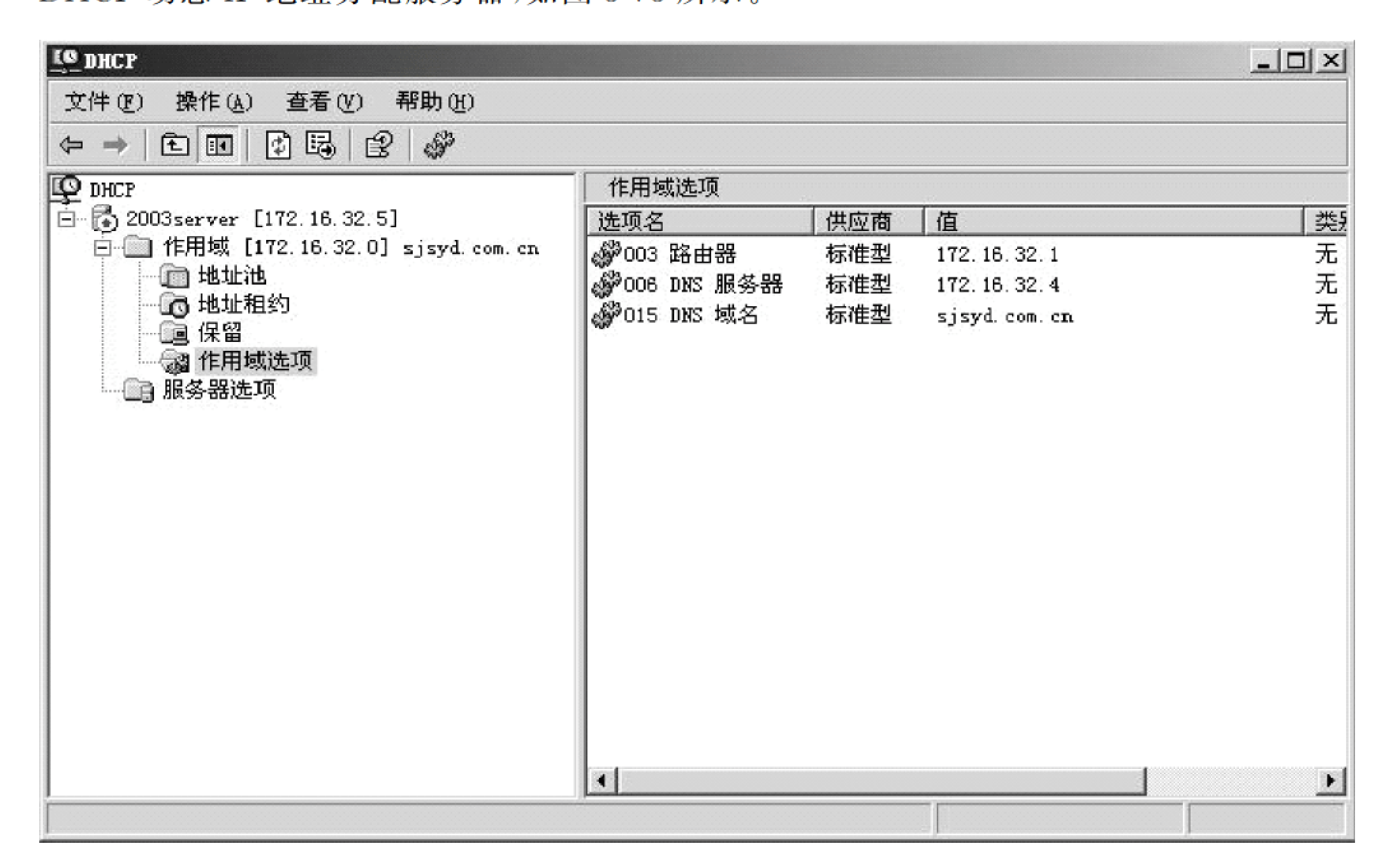


图 3-73　DHCP 服务配置结果

3. Web 服务设置

（1）首先启动 IIS 服务程序，在“Internet 信息服务(IIS)管理器”窗口中，右击“网站”节点下的“默认站点”，在弹出的快捷菜单中选择“新建”→“虚拟目录”命令，如图 3-74 所示。

（2）在弹出的“虚拟目录创建向导”对话框中，根据提示向导一步一步地进行配置。其中，在如图 3-75(a)所示的对话框的“别名”文本框中输入 home，单击“下一步”按钮；在如图 3-75(b)所示对话框的“路径”文本框中输入 C:\www，单击“下一步”按钮。在如图 3-75(c)所示对话框中选择“读取”和“运行脚本(如 ASP)”复选框，使网络用户访问此虚拟目录时只具有对文件的只读权限。

（3）单击“下一步”按钮，完成虚拟目录的创建。当设置好这个虚拟目录后还要给这个目录设置默认的访问文档，方法为：在“home 属性”对话框的“文档”选项卡中，单击“添加”按钮，在弹出的“添加内容页”对话框中输入默认文档名称 index.html 并选择“启用默认内容文档”复选框，如图 3-75(d)所示。

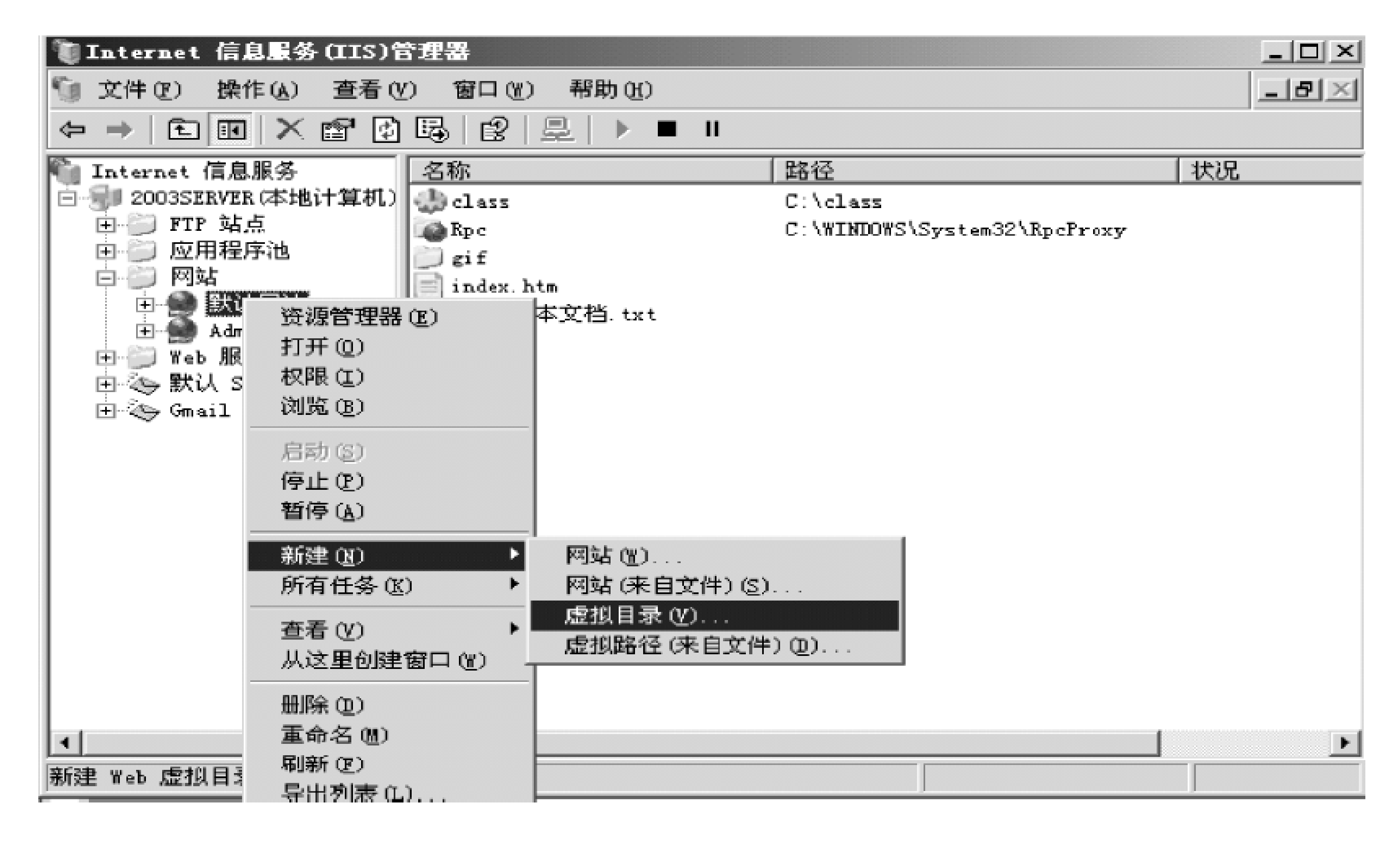
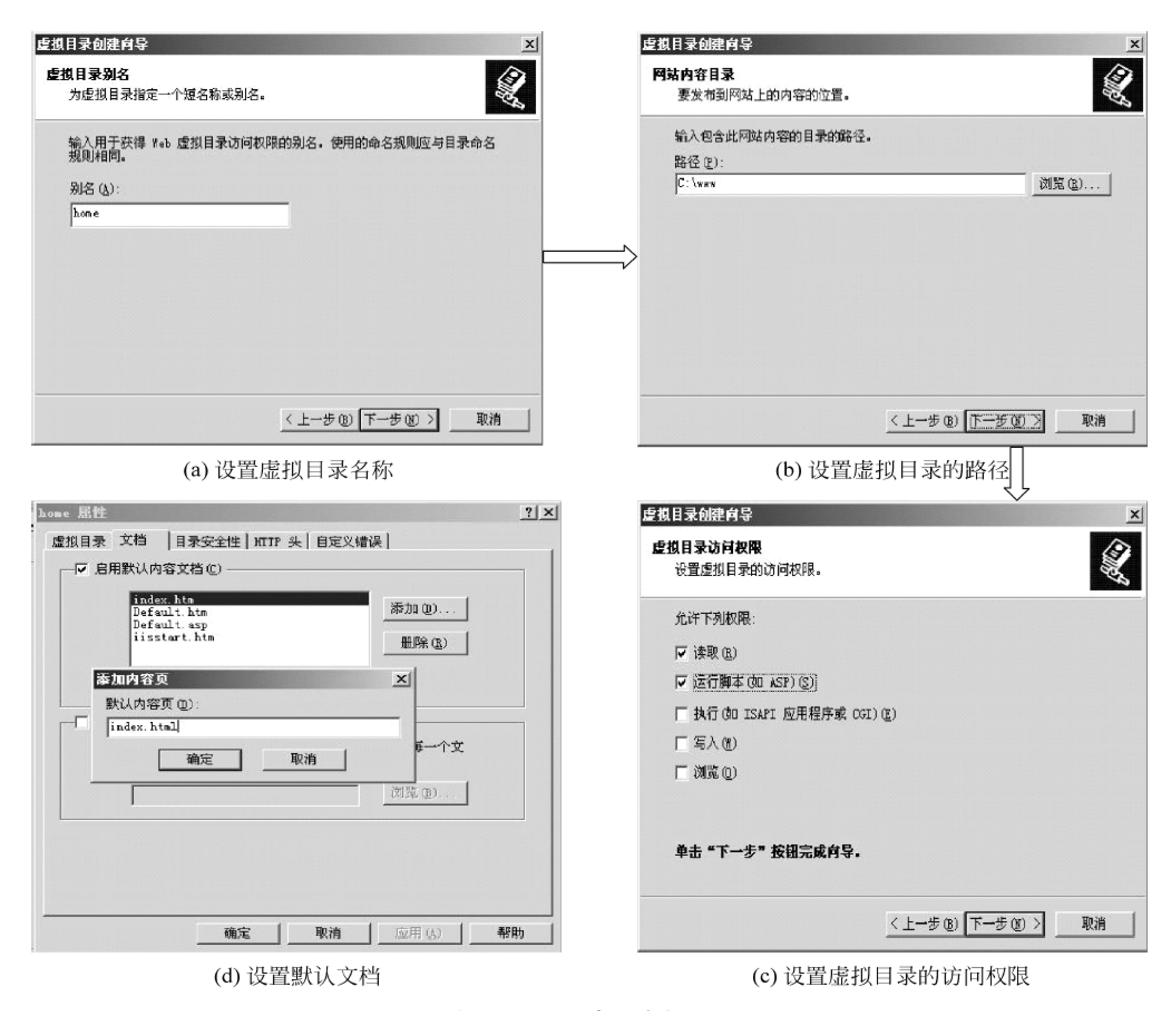


图 3-74　IIS 中建立虚拟目录



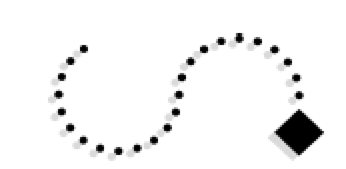
(a) 设置虚拟目录名称

(b) 设置虚拟目录的路径

(d) 设置默认文档

(c) 设置虚拟目录的访问权限

图 3-75　IIS 建立虚拟目录



注意：由于本题目没有涉及 Web 站点的端口问题，所以端口使用系统默认的 80 端口。如果要求使用其他端口，则应在“默认网站”的“属性”对话框的“TCP 端口”文本框中输入要求的端口号。如果题目中要求对站点的目录有修改和写入的权限，还应加入相应用户或用户组的修改和写入权限，否则会出现站点的目录无法修改的错误。

4. FTP 服务设置

(1) 启动 IIS 服务程序，在“Internet 信息服务(IIS)管理器”窗口中，右击“FTP 站点”节点的“默认 FTP 站点”，在弹出的快捷菜单中选择“新建”→“虚拟目录”命令，如图 3-76 所示。

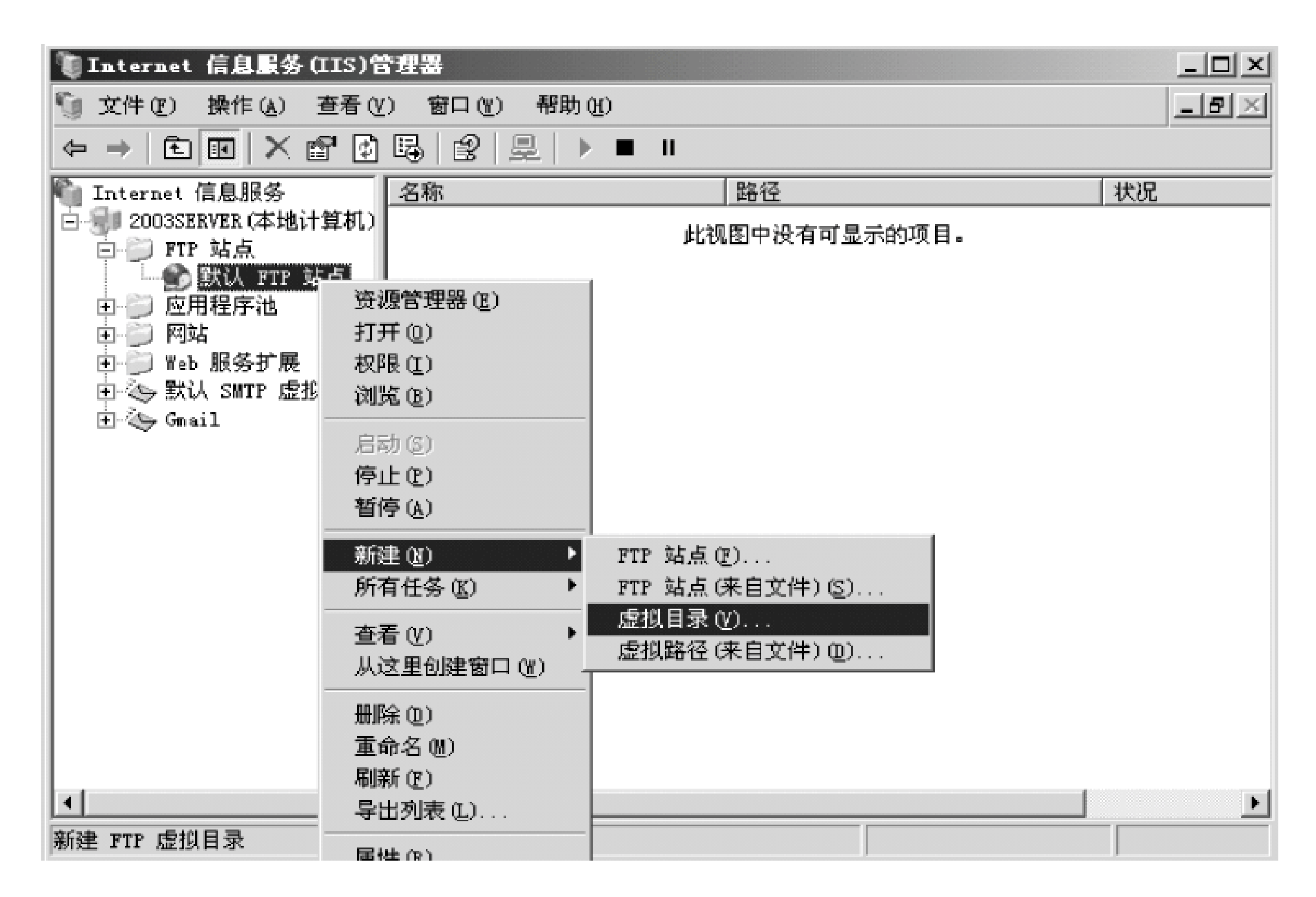


图 3-76　创建 FTP 虚拟目录

(2) 在弹出的“虚拟目录创建向导”对话框中，根据提示进行设置。在弹出的对话框中输入目录的名称 sharefiles，如图 3-77 所示。

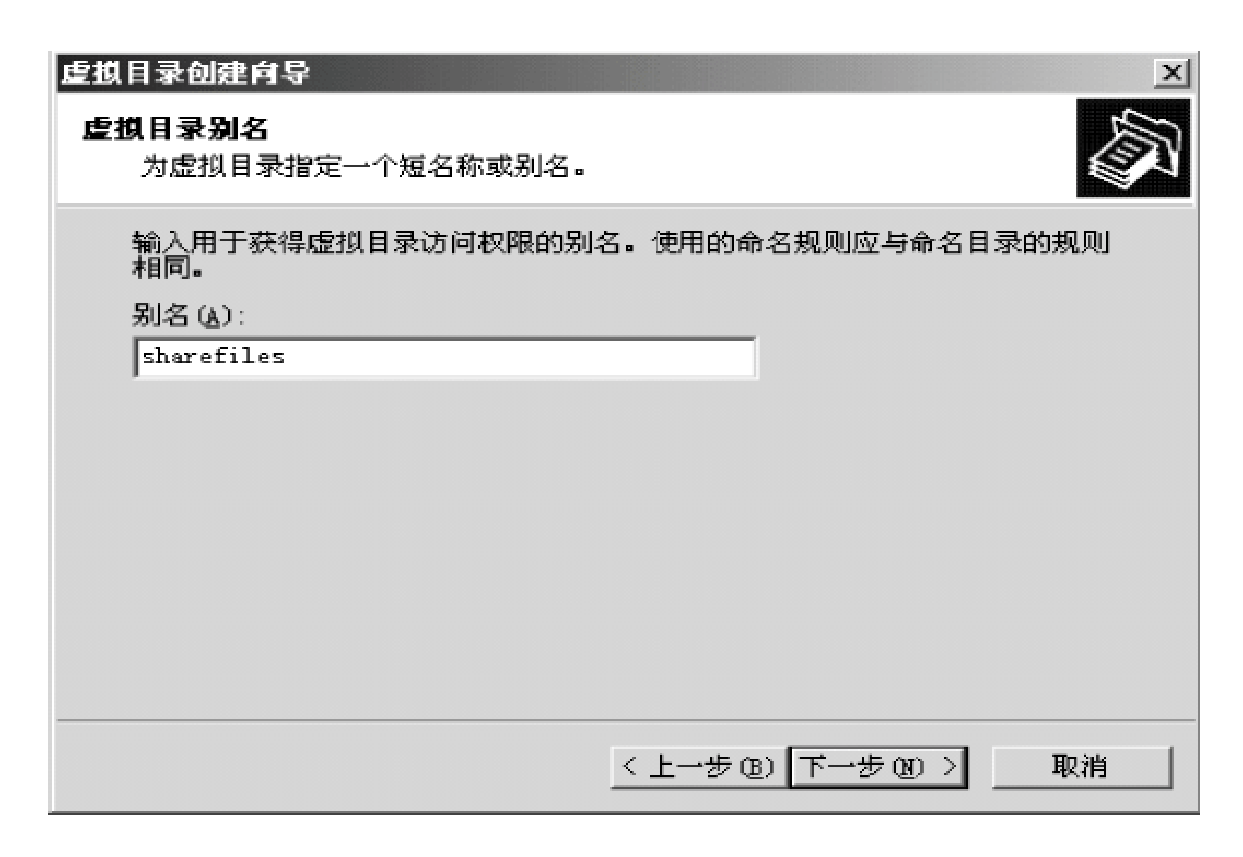


图 3-77　输入虚拟目录的名字

（3）单击“下一步”按钮，在弹出的对话框中输入 sharefiles 虚拟目录对应的本地目录位置，可以在“路径”文本框中输入目录位置 D:\sjsyd. com. cn\ftp，也可以单击“浏览”按钮来查找目录的位置，如图 3-78 所示。



图 3-78　输入虚拟目录对应的本地目录位置

（4）单击“下一步”按钮，在弹出的对话框中设置对目录的操作访问权限，“读取”和“写入”两个复选框都要选择，如图 3-79 所示。

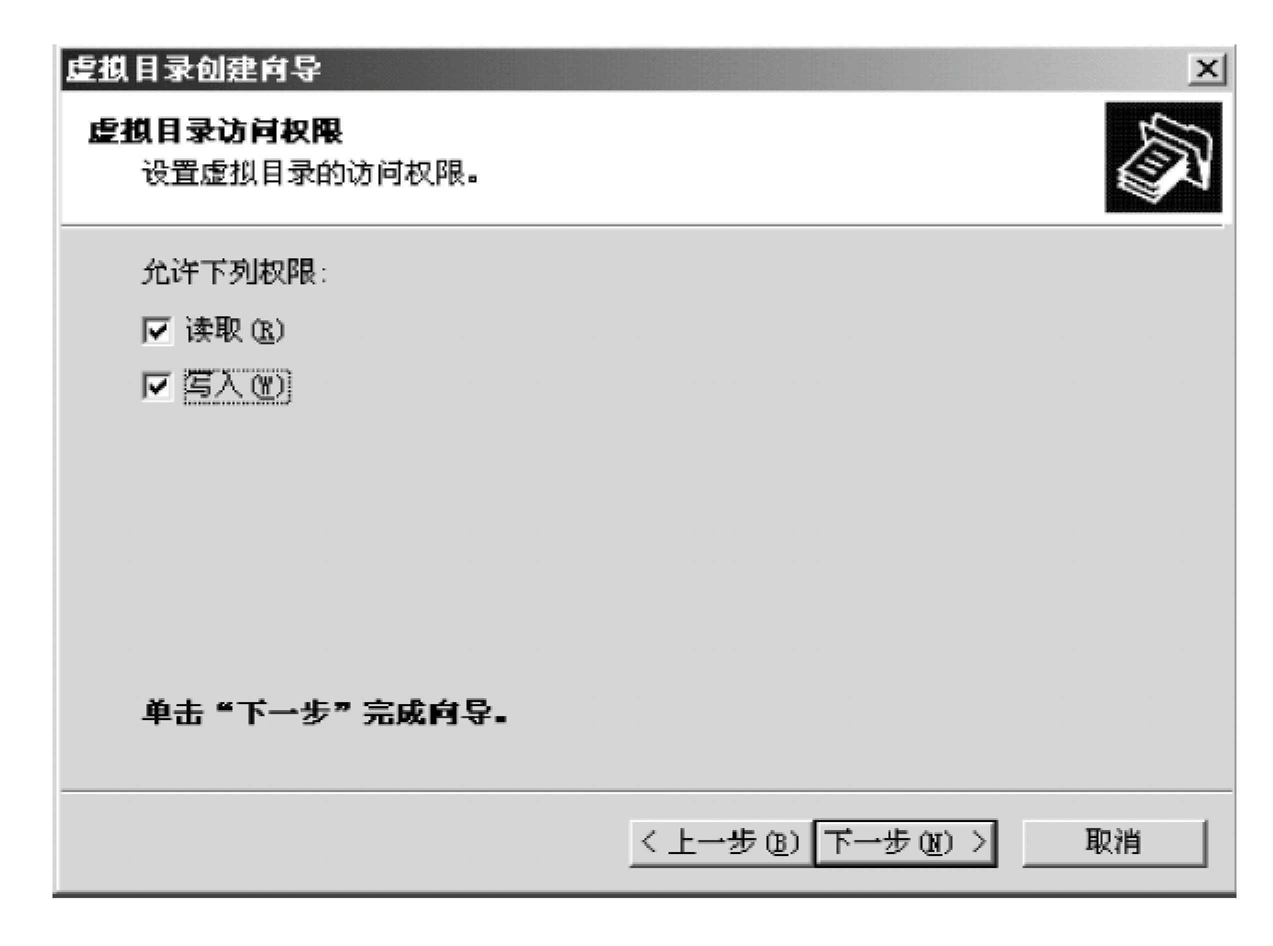


图 3-79　设置访问目录的权限

（5）单击“下一步”按钮，在弹出的对话框中单击“完成”按钮，至此虚拟目录建立完毕。

（6）对 FTP 服务器根的属性进行设置。由于用户一般以匿名方式登录 FTP 服务器，所以要在“默认 FTP 站点属性”对话框的“安全账户”选项卡中进行设置。选择“允许匿名连接”复选框，如图 3-80 所示。单击“确定”按钮，完成 FTP 的设置。用户就可以通过浏览器使用 FTP 协议进行 FTP 服务的应用，如图 3-81 所示。

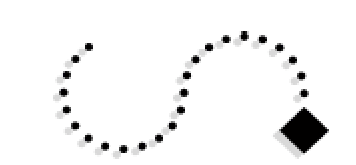




图 3-80　匿名登录的设置



图 3-81　FTP 的应用

3.5　本章小结

本章主要介绍 Windows Server 2003 的网络服务功能，学习如何用相应组件安装、配置网络服务器的方法和技巧，同时介绍了常见的 DNS、DHCP 服务器的工作原理。本章知识的重点是 WWW、DNS、DHCP 及 FTP 的配置与管理。希望通过学习，学会用软件建立应用服务器的一般方法，并能举一反三。

3.6　本章习题

1. 简述 DNS 进行域名解析的工作过程。
2. 简述 DHCP 服务器的工作过程。
3. 用虚拟目录方法，在一个 IP 地址上建两个网站。
4. 用反向域名解析的方法，在一个 IP 地址上建两个网站。
5. 想一想在 Internet 上发布一个网站，要做哪些准备工作？

第 4 章

信息安全

本章内容：

本章将介绍网络安全的知识。首先介绍与信息安全有关的技术：加密技术、密钥管理技术、数字签名技术、数据完整性鉴别技术等。其次介绍信息安全技术在电子商务中的应用。

本章重点：

① 了解信息安全和加密技术的基本概念和简单的密码技术。

② 了解 DES 和 RSA 密码体制。

③ 理解数字签名的基本原理。

④ 了解加密技术在电子商务中的应用。

⑤ 重点掌握加密算法的种类、密钥分配与管理方法及数字签名的实现过程。

随着网络技术的飞速发展，网络已经深入到政府、军事、文教、商业等诸多领域，网络在给人们带来方便、快捷的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门问题等严重威胁着网络的安全。随着人们对计算机网络安全的要求越来越高，这些问题已经引起了普遍关注，成为当今网络技术的一个重要研究课题。

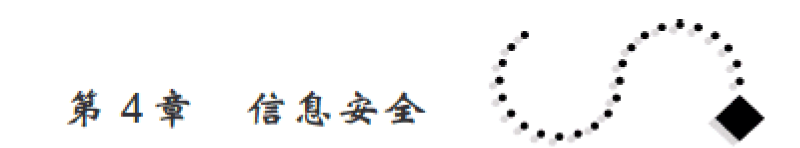
4.1　网络安全概论

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、信息论等多种学科的综合性学科。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义上来说，凡是涉及网络上信息的保密性、完整性、可用性和可控性的理论都属于网络安全的研究领域。

（1）保密性是指信息不泄露给非授权用户。

（2）完整性是指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保



持不被修改、不被破坏和不被丢失的特性。

（3）可用性是指可被授权实体访问并按需求使用的特性，即当需要时能显示信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（4）可控性是指对信息的传播及内容具有控制能力。

1. 网络安全内涵

网络安全包括物理安全、系统安全、信息安全和文化安全，网络安全层次如图 4-1 所示。

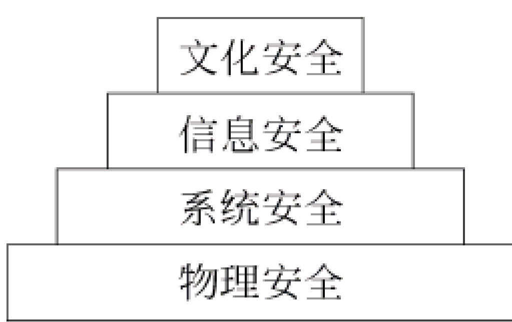


图 4-1　网络安全层次图

（1）物理安全

物理安全是指保护计算机系统的物理设备、网络联接设备、存储介质及其他媒体的安全。对计算机网络与计算机系统的物理设备的威胁，主要表现为自然灾害（包括地震、水灾、火灾、电磁辐射）以及人为操作失误或盗窃等犯罪行为导致的破坏。

危险行为：通信干扰、危害信息的侵入、信号辐射、信号替换、恶劣的操作环境。

防范措施：抗干扰系统、防辐射系统、隐身系统、加固系统、数据备份。

（2）系统安全

系统安全是指保护网络系统、操作系统及数据库系统的安全。系统安全存在的威胁主要表现为对计算机网络与计算机系统可用性与可控性进行攻击，导致网络及计算机不能正常运行。

危险行为：网络被阻塞、非法使用资源、计算机病毒等使得依赖于信息系统的管理或控制体系陷于瘫痪。

防范措施：安装杀毒软件、防止入侵、检测入侵、攻击反应、系统恢复。

（3）信息安全

信息安全是指对计算机存储介质上存放的数据及在网络中传输的数据的安全保护，对所处理的信息机密性与完整性的威胁，主要表现在加密方面。

危险行为：窃取信息、篡改信息、冒充信息、信息抵赖。

防范措施：加密、完整性技术、认证、数字签名。

（4）文化安全

文化安全是指防止有害信息的传播对我国的政治制度及传统文化的威胁，主要表现在舆论宣传方面，防止和控制非法、有害的信息进行传播，避免公用通信网络上大量自由传输的信息失控。

危险行为：淫秽暴力信息泛滥、敌对的意识形态信息涌入、英语文化的“泛洪现象”对民族文化的冲击，互联网被利用作为串联工具，传播迅速，影响范围广。

防范措施：设置网关、监测、控管。

2. 网络系统安全领域存在的威胁

（1）操作系统太脆弱，容易受攻击。使用网络离不开操作系统，操作系统是手工编写的，就可能存在漏洞，有很多网络攻击方式都是针对操作系统的漏洞，入侵计算机来窃取有用信息或阻碍网络信息传输。

（2）系统被攻击时很难及时发现和制止。网络上的攻击方式一般都是比较隐蔽的，

攻击者入侵计算机后造成的影响可能不会马上表现出来。例如，攻击者可能会把计算机病毒放入被攻击的计算机中，在很短的时间里大量复制、感染文件，等待病毒发作。当被攻击者发现系统变慢，文件丢失，甚至系统不能正常启动时，为时已晚。

(3) 有组织有计划的入侵无论在数量上还是在质量上都呈现快速增长趋势。早期的计算机入侵主要是编程高手为了显示自己的水平或者证明程序的弊端，基本上都是个人行为。而现在的入侵比较多的是出于商业或政治上的原因，有组织有计划的入侵可以集中攻击力量，加速入侵的速度，以在更短的时间内造成更大的损失或者获得更多的信息。

(4) 在规模和复杂程度上不断扩展网络而很少考虑其安全状况的变化情况。网络现在已经渗透到各行各业，很多行业对网络的使用只考虑方便性、开放性，并没有考虑总体安全构想，或对网络安全没有足够重视。应该按网络的规模和网络中数据的重要性来设置网络的安全模式和等级。

3. 网络安全中的主要技术

网络在现代工作生活中扮演了重要的角色，改变了人们的工作方式，加快了人们的工作效率。正是因为网络的重要性，所以针对网络的攻击手段随着网络技术的发展也在不断地发展。在网络中采用哪些技术机制才能维护网络的安全呢？

(1) 加密技术

加密是提供信息保密的最核心、最有效的方法。通常按照密钥的类型不同，加密算法可分为对称密钥算法和非对称密钥算法两种。加密算法除了实现信息的保密性之外，还可以和其他技术结合，例如 hash 函数，实现信息的完整性的检验。

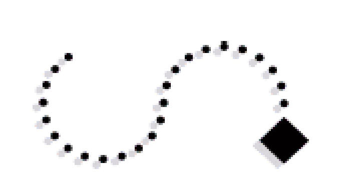
加密技术不仅应用于数据通信和存储，也应用于程序的运行，通过对运行的程序实行加密保护，可以防止软件被非法复制，防止软件的安全机制被破坏。例如利用一些加壳软件，为应用程序加上一个外壳，让软件不能被轻易盗版或复制。

(2) 访问控制技术

访问控制机制是控制进入系统的用户对系统资源的使用范围和访问形式，可以防止未经授权的用户非法使用系统资源，这种访问控制机制不仅可以提供给单个用户，也可以提供给用户组的所有用户。访问控制是通过检查访问者的有关信息来限制或禁止访问者使用资源的技术，分为低层访问控制和高层访问控制。低层访问控制是指通过对通信协议中的某些特征信息的识别和判断，来禁止或允许用户访问的措施。例如，在路由器上设置过滤规则对数据包过滤就属于低层访问控制。高层访问控制包括身份认证和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的。

(3) 数据完整性鉴别技术

数据完整性是指数据是可靠准确的，用来泛指与损坏和丢失相对的数据状态。鉴别是对信息进行处理的人的身份和相关数据内容进行验证，达到信息正确、有效和一致的要求。一般包括口令、密钥、身份、数据等项的鉴别，系统通过对比验证输入的数据是否符合预先设定的参数，从而实现对数据的安全保护。这种鉴别技术主要应用于数据库管理系统中，因为企业经营的重要数据都应该保存在一个可靠的系统中，所以保护好企业数据库的安全是非常重要的工作。数据库系统可以根据不同用户设置不同的访问权限，并对其身份及权限的完整性进行严格识别。



(4) 身份验证技术

身份验证是系统验证用户是否是合法身份的过程。身份验证包括两种：数字签名机制和 Kerberos 系统。

① 数字签名机制

数字签名机制一般采用不对称加密技术(后面会详细介绍)。数字签名可以解决 4 种安全问题。

- 否认：事后发送者不承认文件是他发送的。
- 伪造：有人自己伪造了一份文件，却声称是某人发送的。
- 冒充：冒充别人的身份在网上发送文件。
- 篡改：接收者私自篡改文件的内容。

数字签名机制具有可证实性、不可否认性、不可伪造性和不可重用性。数字签名普遍用于银行、电子商务等系统的身份验证。

② Kerberos 系统

Kerberos 系统是美国麻省理工学院为分布式计算机环境提供的一种对用户双方进行身份验证的方法。Kerberos 系统的安全机制对发出请求的用户进行身份验证，确认其是否是合法的用户，如果是合法的用户，再审核该用户是否有权对他所请求的服务或主机进行访问，其身份是建立在对称加密的基础上的。

(5) 网络防病毒技术

在网络开放的环境下，计算机病毒发展越来越快，并且病毒种类越来越多，也越来越高级复杂，对计算机和网络构成了巨大的威胁。例如，著名的 CIH 病毒让全世界近 6000 万台计算机崩溃，由它直接或间接造成的损失达数亿美元，给社会造成灾难性的后果，因此要重视计算机病毒的防治。网络防病毒技术主要包括预防病毒、检测病毒和清除病毒，具体实现的方法包括对网络服务器中的文件进行频繁地扫描和监测，在工作站上采用防病毒芯片和对网络目录及文件设置访问权限等。

(6) 防火墙技术

防火墙是一个或一组网络设备，包括硬件和软件，在两个或多个网络间保护一个网络不被另一个网络攻击的安全技术。防火墙通常位于内部网或 Web 站点与因特网之间的一个路由器或一台计算机上。防火墙就如同一个防盗门，保证门内的系统安全。在因特网上，通过防火墙来隔离风险区域与安全区域的连接，但不妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信数据，仅让安全、核准的信息进入，抵制对企业构成威胁的数据进入。

防火墙的主要技术包括数据包过滤和应用代理服务。

虽然防火墙技术能在内部网络和外部网络之间建立一道安全屏障，但也存在一定的局限性。防火墙不能完全防范外部刻意的人为攻击，不能防范内部用户攻击，不能防止病毒或受病毒感染的文件的传输。

(7) 入侵检测技术

入侵检测(IDS)通过对计算机网络或计算机系统中若干关键点收集信息，并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测

是防火墙的补充。作为网络安全核心技术之一，入侵检测技术可以缓解访问隐患，弥补防火墙的不足，将网络安全的各个环节有机结合起来，实现对用户网络安全的保护。

4.2　加密技术

为什么要对数据加密呢？对哪些数据加密呢？怎样对这些数据加密？这些都是在网络传输数据时需要知道的问题。存放在计算机系统中的数据每时每刻都受到来自各个方面的威胁。这些威胁轻则会破坏数据的完整性，重则导致数据完全不可用。数据一旦遭到破坏，给数据拥有者带来的损失是无法估量的。有没有一种方法能够较好地保护数据，使其即使遭到攻击也能将损失限制在最小范围内呢？

数据加密和数据备份就是实现这个目标的两种最常用也是最重要的手段。前者通过使原本清晰的数据变得晦涩难懂，从而实现对数据的保护。而后者则在数据遭到破坏后，将数据恢复到最近的一个备份点来尽可能减少数据遭破坏的程度。在数据备份的过程中，数据压缩是一项非常有用的技术，它能够在不影响数据可用性和正确性的前提下大大减少数据所占用的磁盘空间。

几乎任何网络电缆都可能被窃听或监听，攻击者可利用一些网络监听程序或设备截取敏感数据包或其他敏感数据包的备份。假设所有经过网络传输的信息在传输前均被自动地加密，则攻击者将不能完成窃听，网络分析程序收集到的数据包是已加密的数据。如果没有解密密钥，攻击者不能解释该数据，也就不能知道数据里所包含的真实信息。例如，利用加密板或调制解调器之类的硬件，或是利用位于该传输的两个合法末端的软件执行加密或解密。

大多数用户工作的 PC 机都与网络相连，计算机里包含了某些攻击者很想得到的存储宝藏（比如某公司的销售计划、财务报表或相关商业机密等）的硬磁盘。通过网络对该 PC 机的访问几乎是不可阻止的。解决办法是将所有存储于硬磁盘及办公室中的软磁盘上的敏感文件加密。

加密技术是网络信息安全主动的、开放型的防范手段，对于敏感的、重要的数据应采用加密处理，并且在数据传输时也应采用加密传输。本节将着重介绍信息加密技术的一般方法。

4.2.1　数据加密基本概念

数据加密，就是把原本能够读懂、理解和识别的信息（这些信息可以是语音、文字、图像和符号等）通过一定的方法进行处理，使之成为一些晦涩难懂的、不能很轻易明白其真正含意的或者是偏离信息原意的信息，从而保障信息的安全。

下面介绍与数据加密概念相关的几个重要的术语。

（1）明文（Plaintext，记为 P）是信息的原始形式，也就是加密前的原始信息。明文可以是文本、数字化语音流或数字化视频信息等。

（2）密文（Ciphertext，记为 C）是通过数据加密的手段，将明文变换成的晦涩难懂的信息。

（3）加密过程（Encryption，记为 E）是将明文转变成密文的过程。用于加密的这种数

据变换称为加密算法。

（4）解密过程（Dryption，记为 D）是加密的逆过程，即将密文转变成明文的过程。

（5）加密过程和解密过程需要遵循的一个重要原则是明文与密文的相互变换是可逆变换，并且是惟一的、无误差的可逆变换。加密和解密是两个相反的数学变换过程，都是用一定的算法实现的。

（6）密码体制。加密和解密过程都是通过特定的算法来实现的，这一算法称为密码体制。

（7）密钥（Key）是由使用密码体制的用户随机选取的、惟一能控制明文与密文之间变换的关键参数。密钥通常是一随机字符串。

数据加密和解密的过程如图 4-2 所示。

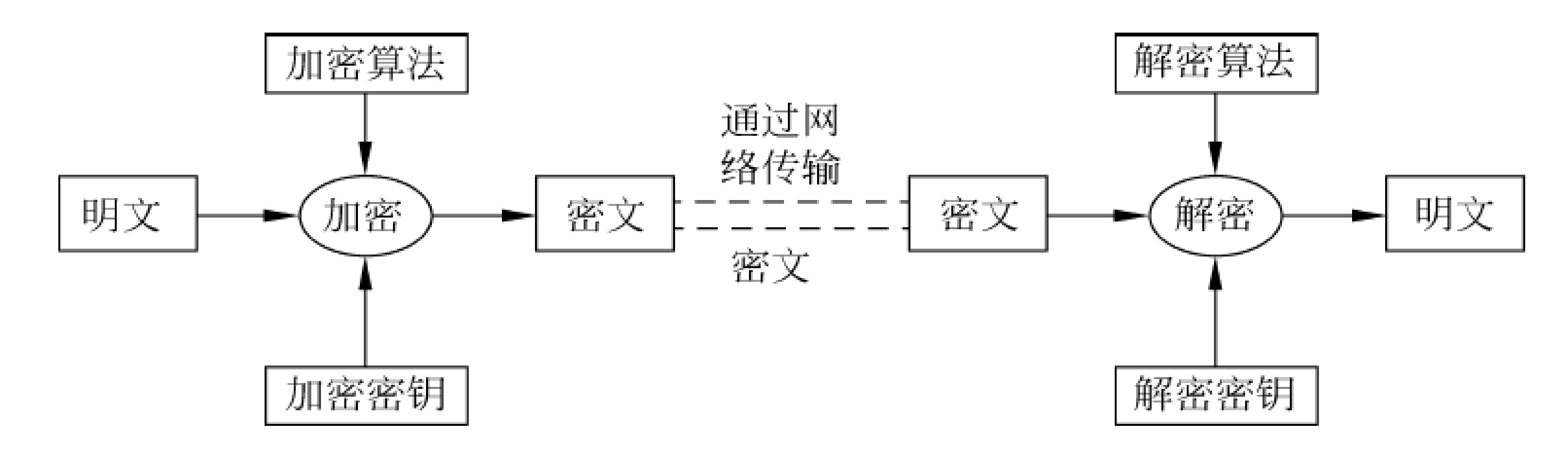


图 4-2　数据加密、解密过程示意图

4.2.2　对称数据加密技术

随着数据加密技术的发展，根据数据加密的方式，可以将密码技术分为对称数据加密技术和非对称数据加密技术。

对称加密又称为密钥加密，是指加密和解密过程均采用同一把秘密钥匙。通信时双方都必须具备这把钥匙，并保证这把钥匙不被泄漏。一旦密钥泄漏，获得密钥的人就可以利用这把钥匙加密或解密，原来加密过的密文就不具有任何保密性了。所以对称密钥加密技术的关键就是要保存好密钥。

通信双方采用对称加密技术进行通信前，双方必须先商定一个密钥，这种商定密钥的过程称为分发密钥。发送方使用这一密钥，并采用合适的加密算法将所要发送的明文转变为密文，然后在网络中传送给接收方，密文到达接收方后，接收方用解密算法（通常是发送方所使用的加密算法的逆运算），利用双方约定的密钥将密文转变为与发送方一致的明文。

采用对称加密技术进行通信的过程如图 4-3 所示。

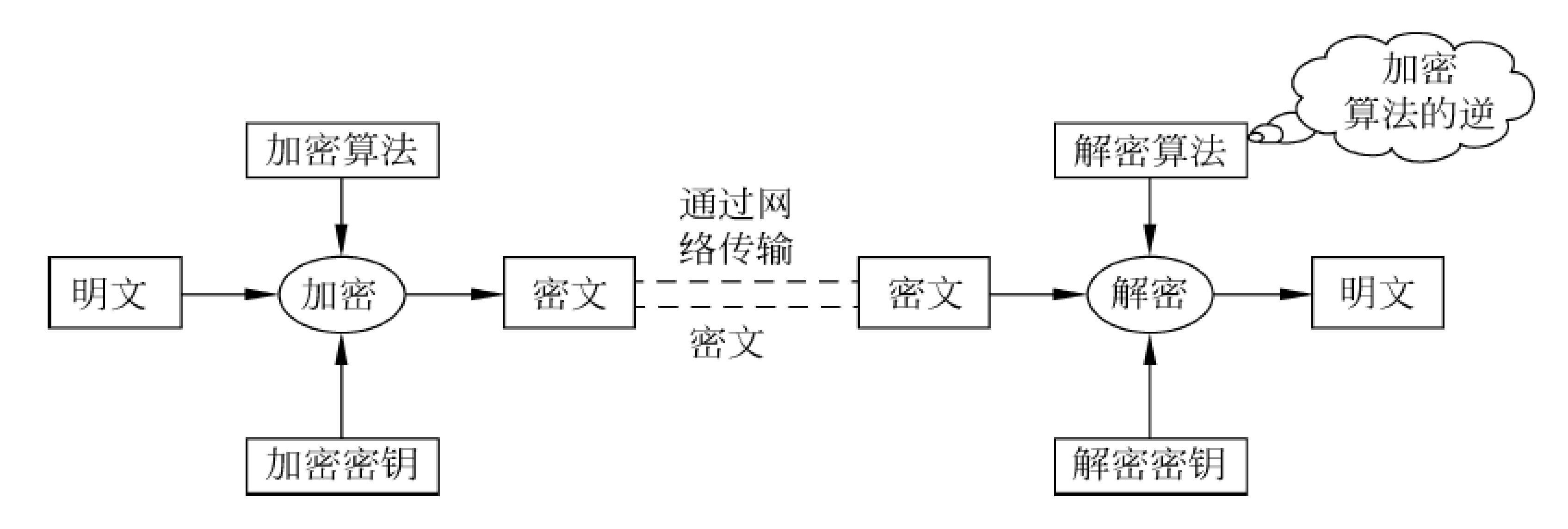


图 4-3　对称加密算法模型

1. 传统的加密技术

(1) 替换密码技术

替换密码技术是将明文字母表中的每个字符替换为密文字母表中的字符,以达到隐藏明文的目的。发送者将明文中每一个字符按照一定规律替换成密文中的另外一个字符。接收者对接收到的密文进行逆替换得到明文。下面介绍两种常用的替换密码算法:单表替换密码和多表替换密码。

① 单表替换技术

如果在替换的过程中明文的一个字符用固定的一个密文字符代替,就称为单表替换技术。最古老的单表替换密码大约出现在公元前 50 年,是由罗马皇帝朱利叶·恺撒发明的一种用于战时秘密通信的方法,这种被称为恺撒密码的技术将字母按字母表的顺序排列,并将最后一个字母和第一个字母相连起来构成一个循环字母表序列,明文中的每个字母用该序列中在它后面的第三个字母来代替,由此形成密文,这种密码也称为循环移位密码。恺撒密码中 26 个英文字母的映射关系如表 4-1 所示。

表 4-1 恺撒密码中 26 个英文字母映射表

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	D	E	F	G	H	I	J	K	L	M	N	O	P
明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

这种映射关系可以用如下函数来表示:

$$F(P) = (P + k)\bmod n$$

其中,P 表示明文字母;

n 表示字符集中字母个数;

k 表示密钥 0。

例如,明文 P=HOW ARE YOU,k=3,则有:

F(H)=(8+3)mod 26=11=K;

F(O)=(15+3) mod 26=18=R;

⋮

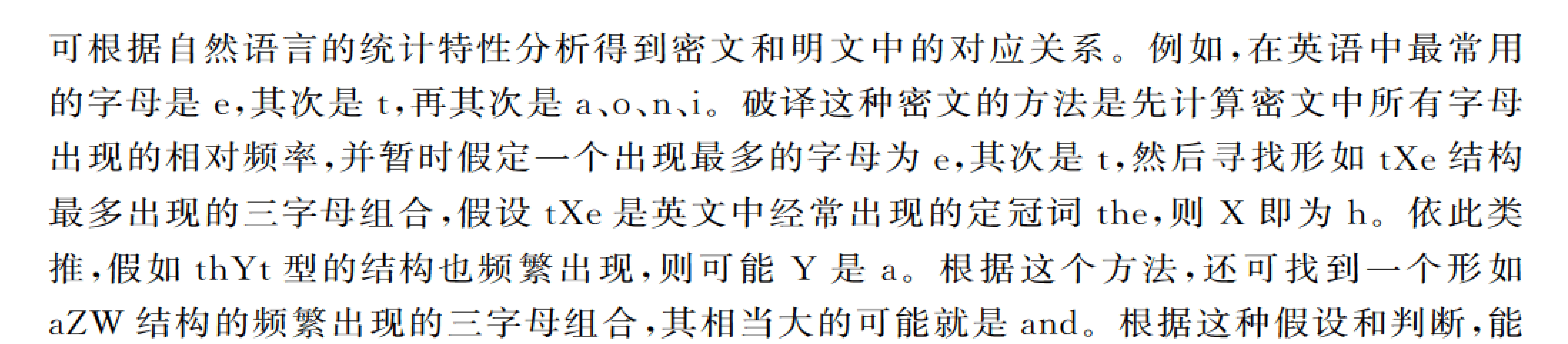
F(U)=(21+3) mod 26 =24=X;

可以得到的密文为:KRZDUHBRX。

对于恺撒密码,解密的方法非常简单,只要依据表中的密文字母和明文字母的对应关系,从密文字母找出相应的明文字母即可。恺撒密码是很容易被破解的,最多进行 25 次尝试就可以得到破解后的明文。由此可见,这种加密算法的安全性很差。

为了提高加密算法的安全性,可以将明文字母和密文字母的映射关系复杂化,将字母表的顺序打乱,使字母之间的映射关系没有规律,即将整个字母表的 26 个字母随意映射到其他字母上。这种改进后的单表加密算法请大家自己分析,看看是否能提高破解的难度,增加加密的安全性。

在明文中英文字母出现的频率是有一定分布规律的,即使打乱了字母表中的顺序,仍


可根据自然语言的统计特性分析得到密文和明文中的对应关系。例如，在英语中最常用的字母是 e，其次是 t，再其次是 a、o、n、i。破译这种密文的方法是先计算密文中所有字母出现的相对频率，并暂时假定一个出现最多的字母为 e，其次是 t，然后寻找形如 tXe 结构最多出现的三字母组合，假设 tXe 是英文中经常出现的定冠词 the，则 X 即为 h。依此类推，假如 thYt 型的结构也频繁出现，则可能 Y 是 a。根据这个方法，还可找到一个形如 aZW 结构的频繁出现的三字母组合，其相当大的可能就是 and。根据这种假设和判断，能初步构成一个试探性明文。

因此，单表替换密码技术的安全性是比较低的，为防止密码被破译，必须使密文中各字母出现的频率趋于平均。如果采用多表替换的密码技术，由于明文中的同一个字符在密文中可以表现为多种字符，所以在密文中消除了明文字母出现频率的规律，大大提高了加密的安全性。

② 多表替换技术

多表替换技术是由多个简单代替表组成。周期替代密码是一种常用的多表替代密码，又称为维吉尼亚(Vignere)密码，这种替代密码是循环地使用有限个字母来实现替代的一种方法。若明文信息为 $p_1p_2p_3\cdots p_n$，采用 m 个字母的序列 $k_1k_2k_3\cdots k_m$ 来实现替换，那么，p_1 将根据字母 k_1 的特性来替换，p_2 将根据字母 k_2 的特性来替换……p_n 将根据字母 k_m 的特性来替换，$p_{(n+1)}$ 又将根据字母 k_1 的特性来替换，$p_{(n+2)}$ 将根据字母 k_2 的特性来替换……可用函数表示为：

$$f(a) = (p + k_i)\text{mod}(n)$$

其中，字母序列 $k_1k_2k_3\cdots k_m$ 就是加密的密钥。

这种加密技术的加密表是把 26 个英文字母进行循环移位后排列在一起，形成 26×26 的方阵，该方阵被称为维吉尼亚表。实际应用时，往往把某个容易记忆的词组当作密钥。维吉尼亚表如表 4-2 所示。

表 4-2　维吉尼亚表

列 / 行	ABCDEFGHIJKLMNOPQRSTUVWXYZ	列 / 行	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ	N	NOPQRSTUVWXYZABCDEFGHIJKLM
B	BCDEFGHIJKLMNOPQRSTUVWXYZA	O	OPQRSTUVWXYZABCDEFGHIJKLMN
C	CDEFGHIJKLMNOPQRSTUVWXYZAB	P	PQRSTUVWXYZABCDEFGHIJKLMNO
D	DEFGHIJKLMNOPQRSTUVWXYZABC	Q	QRSTUVWXYZABCDEFGHIJKLMNOP
E	EFGHIJKLMNOPQRSTUVWXYZABCD	R	RSTUVWXYZABCDEFGHIJKLMNOPQ
F	FGHIJKLMNOPQRSTUVWXYZABCDE	S	STUVWXYZABCDEFGHIJKLMNOPQR
G	GHIJKLMNOPQRSTUVWXYZABCDEF	T	TUVWXYZABCDEFGHIJKLMNOPQRS
H	HIJKLMNOPQRSTUVWXYZABCDEFG	U	UVWXYZABCDEFGHIJKLMNOPQRST
I	IJKLMNOPQRSTUVWXYZABCDEFGH	V	VWXYZABCDEFGHIJKLMNOPQRSTU
J	JKLMNOPQRSTUVWXYZABCDEFGHI	W	WXYZABCDEFGHIJKLMNOPQRSTUV
K	KLMNOPQRSTUVWXYZABCDEFGHIJ	X	XYZABCDEFGHIJKLMNOPQRSTUVW
L	LMNOPQRSTUVWXYZABCDEFGHIJK	Y	YZABCDEFGHIJKLMNOPQRSTUVWX
M	MNOPQRSTUVWXYZABCDEFGHIJKL	Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

例如，使用维吉尼亚密码加密明文 HOW ARE YOU，使用的密钥为 KEY，加密过程如下：给一个信息加密时，只要把密钥反复写在明文下面，每个明文字母下面对应的密钥字母就说明该明文字母应该用维吉尼亚表的哪一行进行加密。

明文：HOW ARE YOU

密钥：KEY KEY KEY

密文：RSU KVC ISS

解密时，以密钥字母选择哪一行，从这一行中找到密文字母，那么密文字母所在的列对应的就是明文字母了。

多表替换密码技术解决了单表替换密码技术中的不安全性。对于同一个明文字母，由于对应的密钥字母不同，将得到不同的密文字母，这样就在密文中消除了明文字母出现频率的规律了。但多表替换密码也不是万无一失的，只要密码分析员拥有足够数量的密文样本，这个算法还是可以破译的，通常可以增加密钥的长度来增加破译的难度。

(2) 置换密码技术

替换密码技术是通过替换明文中的字母来达到隐藏真实信息的目的。置换密码技术是通过改变明文字母的排列次序来达到加密的目的，它把明文中的字母重新排列，字母本身不变，但位置变了。例如，把明文中字母的顺序倒过来写，然后以固定长度的字母组发送或记录。

明文：HOW ARE YOU

密文：UOY ERA WOH

最常用的换位密码是列换位密码。下面来详细说明列换位密码的工作原理。列换位加密算法中，将明文按行排列到一个矩阵中（矩阵的列数等于密钥字母的个数，行数以够用为准，如果最后一行不全可以用不常使用的字符如 X 等填满），然后再按照密钥各个字母大小的顺序排出列号，以列的顺序将矩阵中的字母读出，就构成了密文。

密钥：4312567

明文：CAN YOU UNDERSTAND

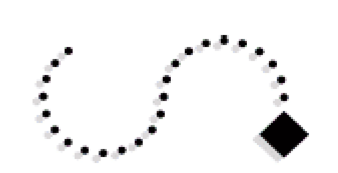
上述明文的列换位加密演示如表 4-3 所示。

表 4-3 列换位加密算法演示

密钥	4	3	1	2	5	6	7
明文	C	A	N	Y	O	U	U
	N	D	E	R	S	T	A
	N	D	X	X	X	X	X

从上面的矩阵中，按照密钥 4312567 的列顺序，按列写出该矩阵中的字母。先从第 1 列中得到 NEX，从第 2 列中得到 YRX，以此类推，得到的密文为：NEXYRXADDCNNOSXUTXUAX。

纯置换密码易于识别，因为它具有与原明文相同的字母频率。对于刚才显示的列变换的类型，密码分析相当直接，将这些密文排列在一个矩阵中，并依次改变行的位量。双字母组和三字母组频率表能够派上用场。



通过执行多次置换，置换密码的安全性能够有较大改观，其结果是使用更为复杂的排列，它不容易被重构。因此，如果前述消息使用相同的算法重加密，则如表 4-4 所示。

表 4-4　二次列换位加密算法演示

密钥	4	3	1	2	5	6	7
明文	N	E	X	Y	R	X	A
	D	D	C	N	N	O	S
	X	U	T	X	U	A	X

密文：XCTYNXEDUNDXRNUXOAASX

为了观察这种双重置换的结果，用原明文消息中的字母所在的位置来指定该字母。在该消息中有 21 个字母 CAN YOU UNDERSTANDXXXXX，传输的字母顺序是：

01　02　03　04　05　06　07

08　09　10　11　12　13　14

15　16　17　18　19　20　21

在进行第一次置换后，得到：NEXYRXADDCNNOSXUTXUAX

03　10　17　04　11　18　02

09　16　01　08　15　05　12

19　06　13　20　07　14　21

它仍有某些规律的结构。但在第二次变换后，得到：XCTYNXEDUNDXRNUXOAASX

17　04　10　03　11　18　02

01　08　16　09　15　05　12

13　20　06　19　07　14　21

此时结构性的排列少得多，密码分析也难得多。

2. 现代对称加密算法 DES

(1) DES 算法及其基本原理

传统的加密方法都要求加密算法和密钥严格保密，这不利于用计算机来实现对信息的加密，因为对每个加密算法都需要编写处理程序，并且该程序必须保密，为此提出了数据加密处理算法标准化的问题。数据加密标准(Data Encryption Standard，DES)是美国国家标准局研究的除国防部以外的其他部门的计算机系统的数据加密标准。虽然从 DES 出现后又产生了许多加密算法，但 DES 仍然是对称加密算法中广泛使用和流行的一种加密算法。

DES 与传统的密码技术的基本原理一样，其密钥是保密的，但加密算法是可以公开的。传统的加密技术一般采用简单的算法并依靠长密钥，而现代的加密技术其密码算法十分复杂，即使破译者得到算法没有密钥也几乎不能破译。DES 是一个分组加密算法，采用两种基本加密组块替代和换位这些技术，通过反复应用来提高加密算法的安全性，经过总共 16 轮的替代和换位后，使密码分析者无法获得该算法一般特性以外更多的信息。DES 以 64 位数据为分组单位对数据加密，64 位一组的明文从算法的一端输入，

64 位的密文从另一端输出。DES 是一个对称算法,加密和解密用的是同一算法(除密钥编排的顺序不同以外)。密钥通常为 64 位数,但每个数有 8 位都用作奇偶校验,可以忽略。密钥可以是任意的 56 位的数,且可在任意时候改变。

DES 加密算法如图 4-4 所示,64 位数据经初始变换后被置换。64 位密钥去掉其第 8、16、24、…、64 位后压缩至 56 位(去掉的那些位被视为奇偶校验位,不含密钥信息),然后就开始各轮运算。64 位数据经过初始置换后被分为左、右各 32 位。56 位的密钥经过左移若干位和置换后取出 48 位密钥子集供不同的加密迭代使用,用作加密的密钥子集记为 K(1)、K(2)、…、K(16)。

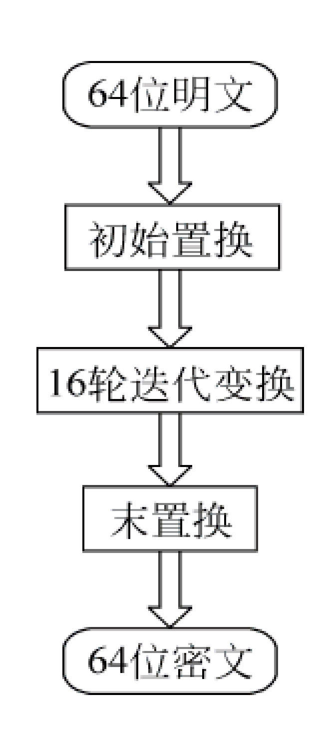


图 4-4　DES 加密算法

在每一轮迭代过程中,先通过重复某些位将 32 位的右半部分数据扩展为 48 位,然后用密钥子集中的一个子密钥K(i)与数据的右半部分进行异或运算,得到的 48 位数通过 S 盒压缩为 32 位。然后再与数据的左半部分的 32 位相异或,其结果作为这一轮迭代的输出数据的右半部分;结合前的右半部分作为这一轮迭代的输出数据的左半部分。这一轮输出的 64 位数据结果作为下一轮的待加密数据,这种迭代要重复 16 次。但最后一轮加密迭代之后,进行逆初始置换运算,它是初始置换的逆运算,最后得到 64 位密文。

(2) DES 解密

DES 算法的解密算法与加密算法可使用相同的算法,二者的惟一不同之处是密钥的次序相反。如果各轮加密密钥分别是 K1、K2、K3、…、K16,那么解密密钥就是 K16、K15、K14、…、K1。为各轮产生密钥的算法也是循环的。

(3) DES 算法的安全性分析

DES 算法是公开的,其安全性完全取决于密钥的安全性。在该算法中,由于经过了 16 轮的代替、置换、异或和循环移动后,使得密码的分析者无法通过密文获得该算法的一般特性以外的更多信息。对于这种算法,破解的惟一办法是尝试所有可能的密钥。对于 56 位长度的密钥,可能的组合达到 $2^{56}=7.2\times10^{16}$种,用穷举法来确定某一个密钥的机会是很小的。

可见,对于 DES 算法的破解是比较困难的。为了更进一步提高 DES 算法的安全性,可以采用加长密钥的方法。例如,IDEA(International Data Encryption Algorithm)算法将密钥的长度加大到 128 位,每次对 64 位的数据组块进行加密,提高了算法的安全性。

4.2.3　非对称数据加密技术

在对称加密算法中,加密算法简单,加密速度快,密钥简短,破解起来比较困难。但是,由于对称加密算法的安全性完全依赖于密钥的保密性,在公开的计算机网络上传送和保管密钥就成为一个严峻的问题。从传统密码出现一直到现代密码学,几乎所有密码编码系统都建立在基本的替代和置换工具的基础上。

公开密钥密码编码学则与以前的所有方法都截然不同。一方面公开密钥算法基于数学函数而不是替代和置换；另一方面更重要的是，公开密钥密码编码学是非对称的，它使用两个不同的密钥，而对称的常规加密则只使用一个密钥。

非对称加密技术，也就是公开密钥算法很好地解决了传送和保管密钥这个问题。它的加密密钥和解密密钥完全不同，不能通过加密密钥推算出解密密钥。之所以称为公开密钥算法，就是因为其公开密钥(Public Key，简称公钥)是公开的，任何人都能通过查找相应的公开文档得到，用它对明文加密，而另一个密钥是私有密钥(Private Key，简称私钥)，是需要保密的，只有得到相应的私有密钥才能解密信息。

1. 公开密钥密码系统的原理

常规加密的密钥分配要求通信双方共享了一个密钥，这个密钥已经以某种方式分配给它们；或者要用一个密钥分配中心。

公开密钥算法用一个公开密钥进行加密，而用一个不同但有关的私有密钥进行解密。仅仅知道密码算法和公开密钥而要确定私有密钥，在计算机上是不可能完成的。另外，公开密钥密码系统还有一个特性，即两个相关密钥中任何一个都可以用作加密而让另外一个用作解密。

公开密钥加密过程的重要步骤如下：

(1) 网络中的每个用户都产生一对用于加密和解密的密钥，即公钥和私钥。

(2) 每个用户都把自己的公钥放进一个登记本或者文件中公布，另一个密钥需要自己妥善保存，不能让第二个用户知道。

(3) 如果 A 想给 B 发送一个报文，就用 B 的公开密钥加密这个报文。

(4) B 收到这个报文后就用自己的私有密钥解密报文，其他所有收到这个报文的人都无法解密它，因为只有 B 才有 B 的私有密钥。

公开密钥算法示意图如图 4-5 所示。使用这种方法，所有用户都可以获得所有的其他用户的公开密钥，而各用户的私有密钥由各用户在本地产生，因此不需要在网络上传送分配。只要各自的私有密钥能保密，收到的通信内容就是安全的。在任何时候，用户都可以更改它的私有密钥并公开相应的公开密钥来替代它原来的公开密钥。

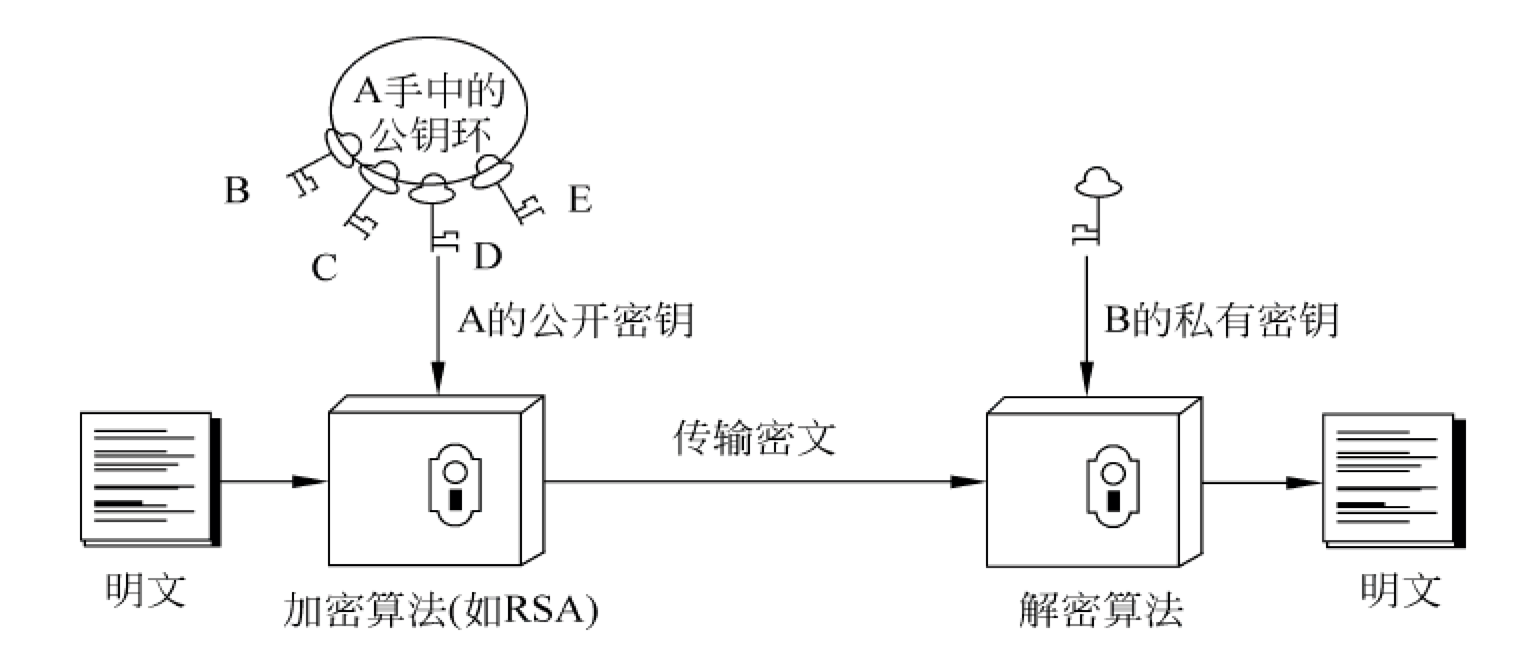


图 4-5　公开密钥算法示意图

对称加密算法和非对称加密算法比较如表 4-5 所示

表 4-5　对称加密算法和非对称加密算法比较

对 称 加 密	非对称加密
运行条件： (1) 加密和解密使用同一个密钥和同一个算法。 (2) 发送方和接收方必须共享密钥和算法。	运行条件： (1) 用同一个算法进行加密和解密，而密钥有一对，其中一个用于加密，另一个用于解密。 (2) 发送方和接收方每个拥有一对相互匹配的密钥中的一个。
安全条件： (1) 密钥必须保密。 (2) 如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的。 (3) 知道所用的算法加上密文的样本必须不足以确定密钥。	安全条件： (1) 两个密钥中的私钥必须保密。 (2) 如果不掌握其他信息，要想解密报文是不可能或者至少是不现实的。 (3) 知道所用的算法加上一个密钥加上密文的样本必须不足以确定另一个密钥。

2. RSA 算法及其基本思想

RSA 算法是在 1977 年由美国麻省理工学院的 Ron Rivest、Adi Shamir 和 Len Adleman 3 位教授研制并于 1978 年首次发表的一种算法，算法的名字取自 3 位教授的名字。RSA 算法是第一个公开密钥算法，是至今为止最为完善的公开密钥算法之一。

RSA 是一种分组密码，其中的明文和密文都是对于某个 n 的从 0 到 $n-1$ 之间的整数。下面通过具体的例子说明 RSA 算法中密钥生成的过程。

(1) 用户 A 秘密选择两个大素数(只能被 1 和自己本身整除的整数)。为了计算方便，假设选择素数 $p=7$ 和 $q=17$。

(2) 计算 $n=p\times q=7\times 17=119$。

(3) 计算出 n 的欧拉函数：$\phi(n)=(p-1)\times(q-1)=6\times 16=96$。

(4) 选择一个 e，它小于 $\phi(n)$ 且与 $\phi(n)=96$ 互素，这样的数非常多，这里取 $e=5$。

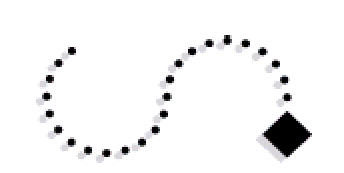
(5) 求出 d，使得 $(d\times e)\bmod\phi(n)=1$，即 $(d\times 5)\bmod 96=1$，可得到 $d=77$。

结果用户 A 得到的公开密钥为 $\{e,n\}$，即 $\{5,119\}$；私有密钥为 $\{d,n\}$，即 $\{77,119\}$。用户 A 得到公开密钥和私有密钥后，把公开密钥告诉用户 B，用户 B 用用户 A 的公开密钥对发送的信息进行加密，然后发送给用户 A。用户 A 再用自己的私有密钥对信息进行解密。

例如，用户 B 将明文为 $M=19$ 的信息发送给用户 A，那么通过如下公式计算得到密文：$C=M^e\bmod(n)=19^5\bmod 119=66$。

用户 B 将密文 66 发送给用户 A，用户 A 在接收到密文信息后，可以使用私钥恢复出明文：$M=C^d\bmod(n)=66^{77}\bmod 119=19$。

从上例中可以看出，从 p 和 q 计算 n 的过程非常简单，但从 $n=119$ 找出 $p=7$、$q=17$ 还是不太容易的。在实际应用中，p 和 q 将是非常大的素数(上百位的十进制数)，那样，通过 n 找到 p 和 q 的难度将非常大，甚至近乎不可能。RSA 算法的安全性基于大数分解的难度。其公钥是一对大素数的函数。从一个公钥和密文中恢复出明文的难度等价于分解两个大素数的乘积。



在使用公开密钥密码系统之前，每个参与者都必须产生一对密钥。这里包括下列任务：

（1）确定两个素数 p 和 q。任何潜在的敌对方都可能知道 $n=pq$ 的值，为了防止通过穷举式方法发现 p 和 q，这些素数必须从足够大的集合中进行选取，另一方面用来找到大素数的方法必须相当有效。

（2）选择 e 或者 d 并且计算另外一个。

3. RSA 算法的安全性分析

RSA 算法的安全性取决于从 n 中分解出 p 和 q 的困难程度。因此，如果找出有效的因数分解的方法，那 RSA 算法的安全性就没有保证了。密码分析学家和密码编码学家一直在寻找有效的因数分解的方法来破解 RSA 算法。随着计算机硬件水平的发展，对一个数据进行 RSA 加密的速度已越来越快，另一方面，对 n 进行因数分解的速度也越来越快，所花费的时间越来越短。

4. 密钥的管理

（1）公开密钥的分配

密钥管理主要处理密钥从产生到最终弃之不用整个过程中的有关问题，包括密钥的产生、存储、导入、分配、保护、丢失和销毁等，密钥管理的主要任务就是保证在公共网络上安全传递密钥而不被窃取。非对称加密系统的一个主要应用是解决对称加密系统中对密钥的保密和分配问题。

分配公开密钥的技术方案主要有下列 4 类。

① 公开宣布。利用一个应用广泛的公开密钥加密算法，比如 RSA，任何参与者都可以将消息用 RSA 算法得到的公开密钥发送给任何一个参与者，或者广播给相关人群，并将参与者的公开密钥附加在他们发送给公开论坛的报文中。这个方法虽然很方便，但存在一个致命的缺陷：任何人都可以依靠并利用这样的公开告示得到公开密钥，缺乏监督机制来约束。如用户 B 可能假装是用户 A，并发送一个公开密钥给另一个参与者 C 或者广播这样一个公开密钥，直到用户 A 发觉了伪造并警告其他参与者的时候，伪造者 B 可能已阅读所有发给 A 的报文，还可以将伪造的密钥用于鉴别。

② 公开目录。通过一个可以得到的公开密钥动态目录就能够取得更大的安全性，对公开目录的维护和分配必须由一个受信任的系统或组织来负责，就像每个参与者手中都有一个公开的电话簿，自己的公开密钥都在这个目录上可供人查询。例如，用户 A 要发送信息给用户 B，先从公开密钥的目录上查到用户 B 的公开密钥。用户 A 就可以用用户 B 的公开密钥把要发送的信息加密再发送给 B。公开目录明显比各个参与者单独进行公示更加安全，但是它仍然有弱点。如果一个敌对方成功地得到或者计算出了目录管理机构的私有密钥，敌对方就可以堂皇地散发伪造的公开密钥，并假装成任何一个参与者并窃听发送给该参与者的报文。如果敌对方篡改管理机构维护的记录也可以达到同样的目的。

③ 公开密钥管理机构。通过更严密地控制公开密钥动态目录中的分配可以使公开密钥分配更安全。假定一个中心管理机构维护一个所有参与者的公开密钥动态目录。另外，每个参与者都知道管理机构的一个公开密钥，而只有管理机构才知道每个

参与者的私有密钥。用户 A 给公开密钥管理机构发送一个带时间戳的报文，其中包含对于 B 的当前公开密钥的请求。管理机构以一个使用它的私有密钥加密的报文进行响应，因为 A 能够使用管理机构的公开密钥解密报文，因此 A 可以确信这个报文来自管理机构，报文中包括 B 的公开密钥。A 存储 B 的公开密钥并使用它加密一个发给 B 的报文。B 可通过同样的方式得到 A 的公开密钥。A 和 B 就可以开始相互之间的秘密信息交互。

公开密钥管理机构可能会由于大量用户请求，而使系统无法同时满足用户的要求，因为用户对于他所希望联系的其他用户都必须借助于管理机构才能得到公开密钥。同样，管理机构所维护的名字和公开密钥目录也可能被篡改。

④ 公开密钥证书。采用这种方法如同直接从公开密钥管理机构得到密钥一样可靠。每个证书包含一个公开密钥以及其他信息，它由一个证书管理机构制作，并发给具有相匹配的私有密钥的参与者。一个参与者通过传输它的证书将其密钥信息传送给另一个参与者，其他参与者可以验证证书是否是管理机构制作的。每个参与者都向证书管理机构提出申请，提供一个公开密钥并请求一个证书。申请必须是面对面的或者是通过某种安全的经过鉴别的方式进行。参与者可以把自己的证书发送给任何其他的参与者，接收者使用管理机构的公开密钥将证书解密对证书进行验证。因为这个证书只能以管理机构的公开密钥进行解读，这就验证了证书的确来自证书管理机构。证书中会告诉接受者证书接受者的名字和公开密钥。最后，时间戳验证了证书的实效性。时间戳防止了参与者的私有密钥被对方获知。A 产生一个新的私有/公开密钥对并向证书管理机构申请一个新的证书，而敌对方将老的证书重放给 B，如果 B 用被泄露的私有密钥对应原公开密钥加密报文，敌对方就可以解读这些报文。

私有密钥的泄露比较像信用卡丢失。持卡人挂失信用卡号码，但是在所有可能的通信方都知道旧的信用卡失效之前仍然有危险。如果一个证书过分陈旧，就可以认为它已经过期。

(2) 秘密密钥的公开密钥加密分配

一旦公开密钥已经分配或者已经可以得到，就可以进行安全通信，阻止窃听、篡改或者其他的攻击行为。因为公开密钥加密的速度相对较慢，很少有用户愿意完全用公开密钥加密进行通信。因此，更合理的做法是将公开密钥加密当作一个分配常规加密所用的秘密密钥的工具。

简单的秘密密钥分配过程：A 先产生一个私有/公开密钥对，然后给 B 传输一个报文，其中包含 A 的公开密钥和一个标识符 ID。B 产生一个秘密密钥 K，并将其用 A 的公开密钥加密后传输给 A。A 用私有密钥来恢复这个秘密密钥。A 和 B 现在就可以使用常规加密用秘密密钥进行安全通信。信息通信完成以后，A 和 B 都丢弃这个秘密密钥 K。这种方式可以将获得密钥的危险减小到最低程度，但是这个方式容易受到主动攻击。如果一个敌对方 E 控制了中间的通信信道，结果是 A 和 B 都得到了 K，并且不知道 K 也被 E 获知。A 和 B 使用秘密密钥进行信息交互时，E 不用主动干预通信信道而只是简单地窃听。因为知道了秘密密钥，E 可以解密所有的报文，而 A 和 B 都不知道有这个漏洞存在。这种简单的协议仅仅在只存在窃听的信道环境中可以使用。

4.3　数字签名和报文鉴别

4.3.1　数字签名

身份验证服务可以确保一个通信是可信的。在诸如产生一个警告或警报信号的单个消息的情况下，鉴别服务的功能是能向接收方保证该消息发送方的真实身份。在一个终端与一台主机连接这样一个正在进行交互的情况下，鉴别服务涉及两个方面。首先，在连接发起时，该服务确保这两个实体是可信的，即每个实体都的确是它们宣称的那个实体。第二，该服务必须确保该连接不被干扰，使得第三方不能假冒这两个合法方中的任何一方来达到未授权传输或接收的目的。

在网络中进行通信，会遇到以下某种攻击。

（1）泄露：将报文内容透露给没有拥有合法密钥的任何人或相关过程。

（2）伪装：敌方伪造一条报文却声称它源自已授权的终端。另外，假的报文接收者对收到报文发回假确认，或者不予接受。

（3）篡改：篡改报文的内容。

（4）抵赖：接收者否认收到某报文或发送者否认发过某报文。

在计算机网络上进行通信不像书信或文件传送那样，可以通过亲笔签名或印章来确认身份。经常会发生这样的情况：发送方不承认自己发送过某一个文件；接收方伪造一份文件，声称是对方发送的；接收方对接收到的文件进行篡改等。那么，如何对网络上传送的文件进行身份验证呢？这就是数字签名所要解决的问题。

一个完善的数字签名应该解决好下面 3 个问题。

（1）当事双方对签名真伪发生争议，应该能够在第 3 方或一个仲裁机构前通过验证签名来确认其真伪。

（2）发送方事后不能否认自己对报文签名。

（3）接收者能够验证签名，其他任何人不能伪造签名，也不能对接收或发送的信息进行篡改、伪造。

满足上述 3 个条件的数字签名技术，就可以对网络上传输的报文进行身份验证。数字签名的实现采用了密码技术，通常采用公钥密钥加密算法实现数字签名，特别是采用 RSA 算法。下面简单介绍一下数字签名的实现思想。数字签名示意图如图 4-6 所示。

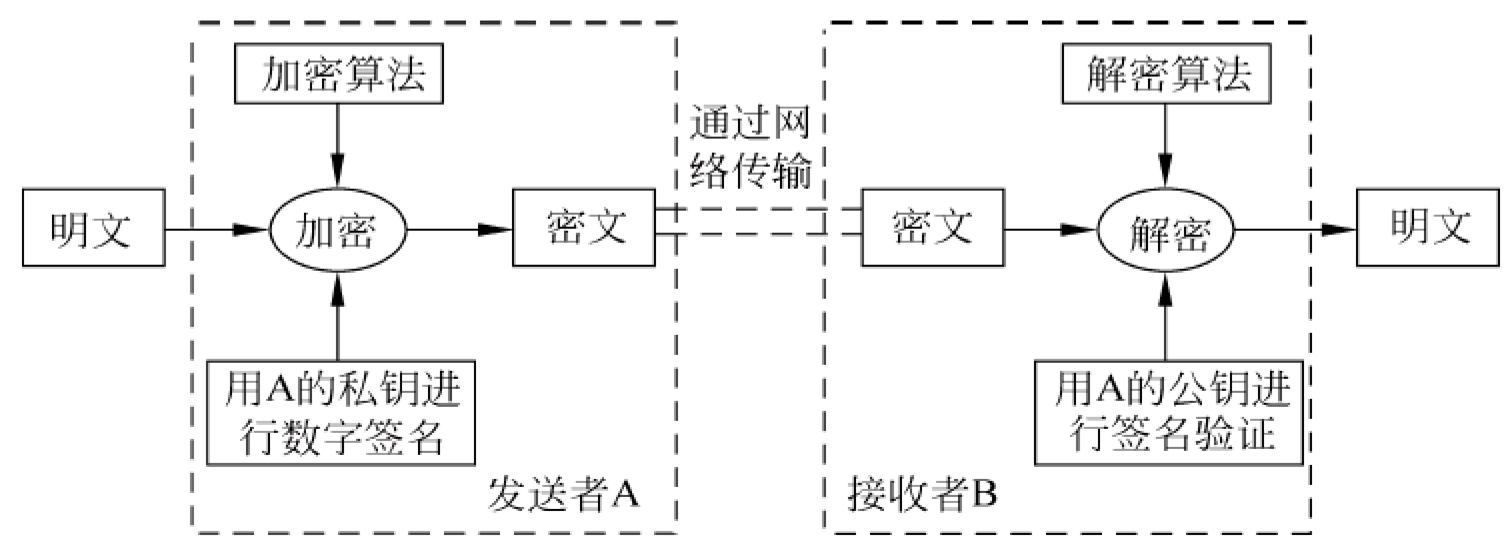
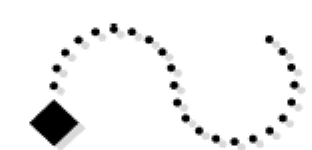


图 4-6　数字签名示意图



报文进行网络传输时，发送者使用自己的私有密钥对报文信息进行加密就形成了签名。将加密的报文发送给接收者。接收者在接收到加密的报文后，采用已知发送者的公钥对报文进行解密运算，就可以核实签名。

上述过程实现了对报文信息的数字签名，但报文并没有进行加密，如果其他人截获了报文并知道了发送者的身份，就可以查阅文档得到发送者的公钥，从而获取报文的内容。

为了达到加密的目的，在将已签名的报文发送出去之前，先用接收方的公钥对报文进行加密，接收方在接收到报文后先用私钥对报文进行解密，然后再用发送方的公钥验证发送方的签名。这样，就可以达到加密和签名的双重效果。

4.3.2 报文鉴别和 MD5 算法

在计算机网络安全领域中，防止信息被窃听所采取的措施是对发送的信息进行加密，而防止信息被篡改和伪造需要使用报文鉴别技术。鉴别是验证通信对象是原定的发送者而不是冒名顶替的一种技术。报文鉴别保证通信的接收方能够验证所收到的报文的真伪。

报文的安全性可以通过报文加密来实现。在特定的网络应用中，许多报文并不需要加密，但是要求发送的报文是完整的、没有被篡改和不是伪造的。例如，在网络上发布一个公告，就不需要加密，而只要保证其是完整的，没有被篡改。对不需要保密的报文进行加密和解密，将会浪费计算机的系统资源和增加运算时间。因此，可使用相对简单的报文鉴别算法来达到目的。

目前，大多使用报文摘要（Message Digest，MD）算法来进行报文鉴别，其主要原理如图 4-7 所示。

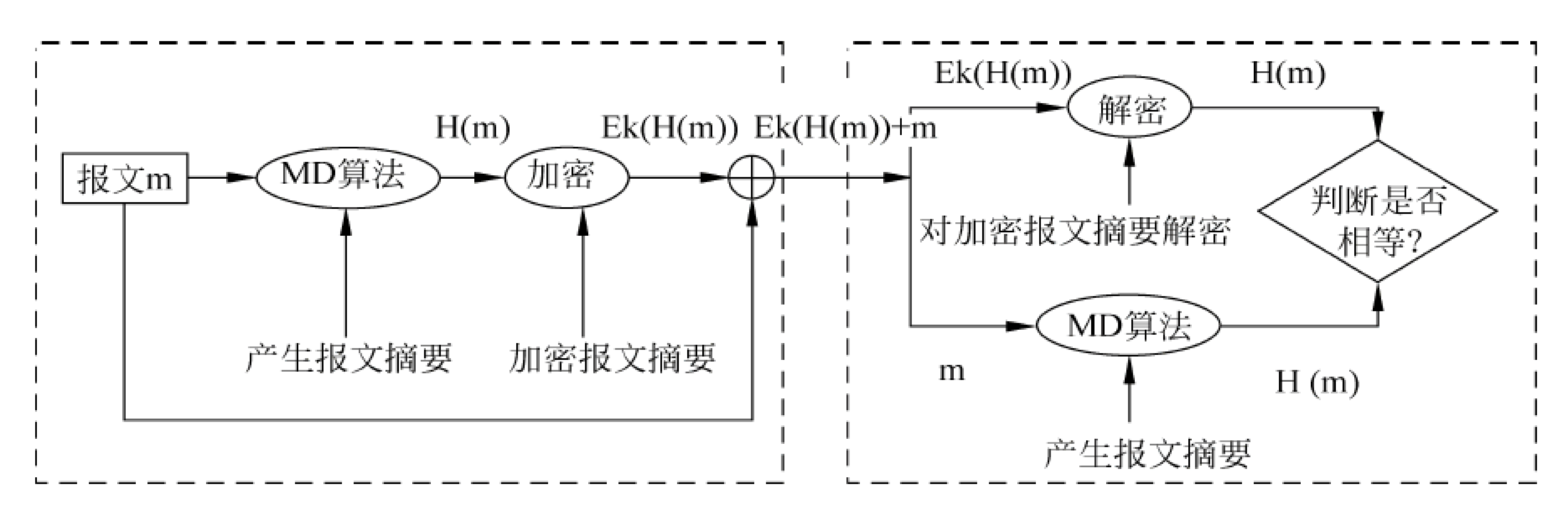
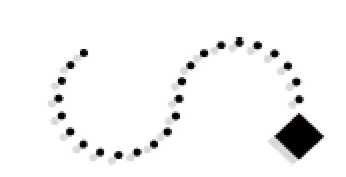


图 4-7 报文摘要示意图

对报文摘要示意图说明如下：

- 发送方将待发送的可变长报文 m 经过 MD 算法运算得出固定长度的报文摘要H(m)。
- 使用密钥 K 对 H(m)生成报文摘要密文 Ek(H(m))附加在报文 m 之后一起发送。
- 在接收方收到报文 m 和报文摘要密文 Ek(H(m))之后，将报文摘要密文 Ek(H(m))解密还原成 H(m)。
- 同时接收方将收到的报文 m 经过 MD 算法运算得出的报文摘要与 H(m)比较是否相同，若不相同则可断定收到的报文不是发送方产生的。



报文摘要的优点：对短的固定长度的报文摘要 H(m)进行加密比对整个报文 m 进行加密的计算效率要高得多。

要实现报文 m 和加密的报文摘要 Ek(H(m))在一起是不可篡改和伪造的，是可鉴别和不可抵赖的，MD 算法必须满足两个条件。

(1) 对于给定的一个报文摘要值 x，若想找到一个报文 y，使得 H(y)＝x，在计算上不可行，或者想从算法上得到结果，其时间代价之高是无法承受的。

(2) 两个不同报文产生同样的报文摘要在计算上是不可行的。

这两个条件表明：(m，H(m))是发送方产生的报文和报文摘要，攻击者不可能仿造另一个报文 m′，使得 H(m′)＝H(m)，从而达到报文鉴别的目的。同时发送方可以对 H(m)进行数字签名，使报文成为不可抵赖的。

报文摘要一般采用散列函数(Hash Function)实现，目前用得最为广泛的是 MD5 报文摘要算法。

MD5 属于一种被称之为报文摘要算法的哈希函数，MD5 系统的定义是算法以一个任意长信息作为输入，产生一个 128 位的“指纹”或“摘要信息”。MD5 系统主要是用在数字签名和报文鉴别中。

MD5 算法是对需要进行摘要处理的报文信息块按 512 位并行处理的。首先将需要进行摘要处理的报文信息块进行填充，使信息报文的长度等于 512 的倍数。填充时首先在需要进行摘要处理的报文信息块后填充 64 位的信息长度，其首位为 1，其他位全为 0；然后对信息报文依次处理，每次处理 512 位，每次进行 4 轮 16 步总共 64 步的信息变换处理，每次输出结果为 128 位，然后把前一次的输出作为下一次信息变换的输入初始值(第一次初始值算法已经固定)，这样最后输出一个 128 位的哈希摘要结果。目前 MD5 被认为是最安全的报文摘要算法之一，已经在很多应用中被当成标准使用。

MD5 提供了一种单向的哈希函数，是一种校验和报文鉴别工具。MD5 将一个任意长的字符串作为输入，产生一个 128 位的报文摘要，附在信息报文后面，以确保鉴别报文以防篡改。MD5 认为对两个不同报文产生同样的报文摘要在计算上是不可行的，并且一个已给定的报文摘要对另一个报文产生同样的报文摘要也是不可计算的。MD5 的散列结果为 128 位。如果采用穷举法攻击，每秒 10 亿条明文的计算量需要计算约 10 年。

MD5 算法是对付特洛伊木马程序(有关特洛伊木马的知识将在后面的相关章节中详细介绍)的非常有效的工具。通过 MD5 算法计算每个文件的数字签名可检查文件是否被更换或是否与原来的一致。

4.4　信息安全技术在电子商务中的应用

网络在人们日常生活和工作中的应用越来越广泛，作为 21 世纪的主要经济形式——电子商务，将给全世界经济带来巨大的变革。电子商务可以大幅度降低交易成本，增加贸易机会，简化贸易流程，提高贸易效率，改善物流环节，推动企业和国民经济结构的改革。电子商务是一个机遇和挑战共存的新领域，这种挑战大多数来源于对使用的安全技术的信赖。如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，是商家和

 用户都十分关注的问题。安全问题已成为电子商务的核心问题。要加强电子商务的安全,需要企业本身采取更为严格的管理措施,需要国家建立健全的法律制度,更需要有科学的、先进的信息安全技术。

4.4.1 电子商务的安全概述

当今世界上最著名的阿里巴巴网站是全球最大的网上贸易市场和商人社区,为来自220多个国家和地区的760多万企业和商人提供网上商务服务。很多中小企业通过电子商务获得了巨大商机,但也有些企业由于网上交易陷入欺诈陷阱。所以要充分认识到电子商务为企业带来的益处,但同时也要看到电子商务目前发展的不完善性。

1. 电子商务的基本结构和流程

目前世界上通过因特网进行电子商务的个人和企业不断增加,但如果把信用卡的号码、有效期限、使用者姓名等重要信息直接通过网络传送,每个人都会担心,个人信息会不会泄漏,会不会有人盗用信用卡等。因此必须建立一个能够安全可靠地进行电子商务数据交换的系统。

电子商务的服务模式主要有：企业内部之间、企业和企业之间、企业与消费者之间等。企业—企业和企业—消费者之间电子商务的交易过程是有差异的,和传统的商务活动不同的是,在电子商务的流程中,企业、消费者、银行和第三方交易平台、认证体系、物流配送体系等积极参与交易的整个过程。虽然电子商务的发展是不可阻挡的潮流,但是目前在发展过程中还面临一些基本问题,也称为电子商务发展过程中的七大瓶颈,它们分别是认证体系、安全保障、在线支付安全、物流配送体系、互联网络的带宽、法律环境以及协同作业平台问题。企业在实施电子商务时必须正视这些问题,并协同寻求解决之道。

传统企业要根据电子商务的发展趋势确立自己的因特网发展策略：通过因特网建立全新的商业模式,将商业行为的主导权从卖方转移到了买方,使消费者拥有更全面的信息、更多的选择和更强大的交易工具,在交易中逐步占据主动地位。电子商务需要全新的商业理念。对一些企业来说,电子商务的应用,简单地使用Web是不够的,必须重新考虑企业的电子商务应用环境、原有的信息管理技术和业务流程。因特网可以使企业以从前不可想象的方式,将自身运作和其他组织整合在一起。

网上交易流程有很多种类型,主要分为网络商品直销和网络商品中介交易这两种基本的流程。

(1) 网络商品直销的流程

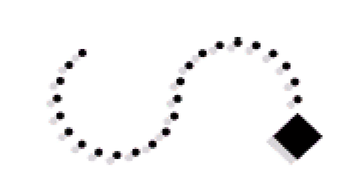
网络商品直销是指消费者和生产者或者是需求方和供应方直接利用网络形式所开展的买卖活动。这种在网上的买卖交易最大的特点是供需直接见面,环节少,速度快,费用低廉。

① 消费者在因特网上查看企业和商家的主页(HomePage);

② 消费者通过购物对话框填写姓名、地址、商品品种、规格、数量、价格;

③ 消费者选择支付方式,如信用卡、借记卡、电子货币、电子支票等;

④ 企业或商家的客户服务器接到定单后检查支付方的服务器,确认汇款额是否被认可;



⑤ 企业或商家的客户服务器确认消费者付款后，通知销售部门送货上门；

⑥ 消费者的开户银行将支付款项传递到信用卡公司，并由信用卡公司负责发给消费者收费单。

在上述过程中，认证中心（CA）作为第三方，确认在网上经商者的真实身份，保证了交易的正常进行。

网络商品直销的诱人之处在于它能够有效地减少交易环节，大幅度地降低交易成本，从而降低消费者所得到的商品的最终价格。消费者只需输入厂家的域名，访问厂家的主页，即可清楚地了解所需商品的品种、规格、价格等情况，而且，该商品厂家主页上的价格最接近出厂价，这样就有可能达到出厂价格和最终价格的统一，从而使厂家的销售利润大幅度提高，竞争能力不断增强。

网络商品直销的不足之处主要表现在两个方面。第一，购买者只能从网络广告上判断商品的型号、性能、样式和质量，对实物没有直接的感知，在很多情况下可能产生错误的判断；而某些厂商也可能利用网络广告对自己的产品进行不实的宣传，甚至可能打出虚假广告欺骗顾客。第二，购买者利用信用卡进行网络交易，不可避免地要将自己的密码输入计算机，由于新技术的不断涌现，犯罪分子可能利用各种高新科技的作案手段窃取密码，进而盗窃用户的钱款，这种情况不论是在国外还是在国内均有发生。

（2）网络商品中介交易的流程

网络商品中介交易是通过网络商品交易中心，即虚拟网络市场进行的商品交易，如阿里巴巴，或购物网站如易趣网等。在这种交易过程中，网络商品交易中心以因特网为基础，利用先进的通信技术和计算机软件技术，将商品供应商、采购商和银行紧密地联系起来，为客户提供市场信息、商品交易、仓储配送、货款结算等全方位的服务。

买卖双方各自的供需信息通过网络告诉网络商品交易中心，网络商品交易中心通过信息发布服务向交易的参与者提供大量的、详细准确的交易数据和市场信息。

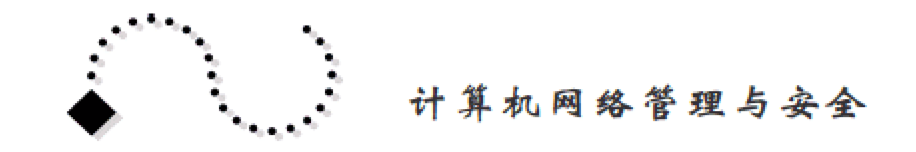
买卖双方根据网络商品交易中心提供的信息，选择自己的贸易伙伴。网络商品交易中心从中撮合，促使买卖双方签订合同。

买方在网络商品交易中心指定的银行办理转账付款手续。

网络商品交易中心在各地的配送部门将卖方货物送交买方。

通过网络商品中介进行交易具有许多突出的优点。首先，网络商品中介为买卖双方展现了一个巨大的世界市场，这个市场网络储存了全世界的几千万个品种的商品信息资料，可联系千万家企业和商贸单位。每一个参加者都能够充分地宣传自己的产品，及时地沟通交易信息，最大限度地完成产品交易。各种网络商品中介机构通过网络彼此连接起来，进而形成全球性的大市场，目前这个市场正以每年 70％的速度递增。其次，网络商品交易中心作为中介方可以监督交易合同的履行情况，有效地解决在交易中买卖双方产生的各种纠纷和问题。最后，在交易的结算方式上，网络商品交易中心采用统一集中的结算模式，对结算资金实行统一管理，有效地避免了多形式、多层次的资金截留、占用和挪用，提高了资金风险防范能力。

网络商品中介交易的方式目前存在的主要问题是，现在使用的合同文本还是以买卖双方签字交换的方式完成，如何过渡到电子文本合同，并在法律上得以认可，尚需解决有



关技术和法律问题。

2. 电子商务安全因素与安全技术

(1) 电子商务的安全要素

① 有效性。电子商务以电子形式取代了纸张,那么如何保证这种电子形式的贸易信息的有效性则是开展电子商务的前提。电子商务作为贸易的一种形式,其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此,要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防,以保证贸易数据在确定的时刻、确定的地点是有效的。

② 机密性。电子商务作为贸易的一种手段,其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务建立在一个较为开放的网络环境上(尤其因特网是更为开放的网络),维护商业机密是电子商务全面推广应用的重要保障。因此,要预防非法的信息存取和信息在传输过程中被非法窃取。

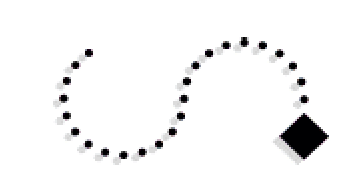
③ 完整性。电子商务简化了贸易过程,减少了人为的干预,同时也带来维护贸易各方商业信息的完整和统一的问题。由于数据输入时的意外差错或欺诈行为,可能导致贸易各方信息的差异。此外,数据传输过程中信息的丢失、重复或传送次序的差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略,保持贸易各方信息的完整性是电子商务应用的基础。因此,要防止对信息的随意生成、修改和删除,同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。

④ 可靠性/不可抵赖性/可鉴别性。电子商务直接关系到贸易双方的商业交易,确定要进行交易的贸易方正是交易所期望的贸易方是保证电子商务顺利进行的关键。在传统的纸面贸易中,贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或加盖印章来鉴别贸易伙伴,确定合同、契约、单据的可靠性并预防抵赖行为的发生,这也就是人们常说的白纸黑字。在无纸化的电子商务方式下,通过手写签名和加盖印章进行贸易方的鉴别是不可能的。因此,要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。

⑤ 即需性。即需性是防止延迟或拒绝服务,即需安全威胁的目的就在于破坏正常的计算机处理或完全拒绝服务。在电子商务中,延迟或消除一个消息会带来灾难性的后果。例如,某个用户在上午 10 点向在线的股票交易公司发一个电子邮件委托购买 1000 股 IBM 公司的股票,假如这个邮件被延迟了,股票经济商在下午 2 点半才收到这封邮件,这时股票已经涨了 15%,这个消息的延迟就使该用户损失了交易额的 15%。

⑥ 身份认证。身份认证是指交易双方可以相互确认彼此的真实身份,确认对方就是本次交易中声称的真正交易方。认证是证实一个声称的身份或者角色,如用户、机器、节点等是否真实的过程。身份认证过程为授权和审计所必需,也是实现授权、审计的访问控制过程运行的前提,是计算机网络安全系统不可缺少的组成部分。

⑦ 审查能力。根据机密性和完整性的要求,应对数据审查的结果进行记录。审查能力是对每个经授权的用户的活动的惟一标识和监控,以便对其所使用的操作内容进行审



计和跟踪，防止当贸易一方发现交易行为对自己不利时可以拒绝电子商务行为。

（2）电子商务中使用的信息安全技术

为了保证电子商务交易的安全，在电子商务中使用了各种信息安全技术。

① 加密技术。加密技术是电子商务中采用的主要安全措施，交易双方可根据需要在信息交换阶段对传送的信息加密。

② 密钥管理技术。对称密钥管理是基于共同保护秘钥来实现的，采用对称加密技术的双方必须采用安全可靠的方式来保护密钥，同时要设定防止密钥泄漏和更改密钥的程序。使用公开密钥的交易双方可以使用证书来交换公开密钥。数字证书能够起到标识交易双方的作用，是目前电子商务中使用较为广泛的技术之一。

③ 数字签名。数字签名是公开密钥加密技术的另一种应用。报文的发送方从报文信息中生成一个 128 位的散列值，发送方用自己的私有密钥对这个散列值进行加密来形成发送方的数字签名，通过数字签名能够实现对原始报文的不可抵赖性。

④ 防火墙技术。防火墙主要用来隔离内部网络和外部网络，保护内部网不受外部网的攻击。目前防火墙主要有包过滤技术和应用网关—代理服务器。包过滤技术是在网络层中按照过滤规则对数据包实施有选择的通过。应用网关—代理服务器可针对网络应用服务协议即数据过滤协议进行存取控制，并且能够对数据进行分析并形成相关的报告。

⑤ CA 技术。认证机构体系 CA 是指一些不直接从电子商务贸易中获利的、受法律保护的、可信任的权威机构，CA 负责发放和管理电子证书，使网上通信的各方能互相确认身份。CA 的基本功能有：接收注册请求，处理、拒绝/批准请求，颁发证书。在实际运用中，CA 由大家都信任的机构担当，如中国数字认证中心等。

4.4.2　电子商务中使用的安全协议

在电子商务发展中，最关键的问题是如何在开放的公开网络上保证交易的安全性，即如何构筑一个安全的交易模型。一个安全的电子交易模型应该包括 5 个方面的内容：数据保密、身份认证、数据完整性、防抵赖性和访问控制。目前，有两种安全在线支付协议被广泛采用，即 SSL 协议和 SET 协议。

1. SSL 协议

SSL（Secure Socket Layer，安全套接层）协议是网景（Netscape）公司提出的一种基于 Web 应用的网络安全通信协议，它包括服务器认证、客户认证、SSL 链路上的数据完整性和 SSL 链路上的数据保密性，主要采用公开密钥体制和 X.509 数字证书技术来提供数据传输的安全性保证。对于电子商务应用来说，SSL 协议可保证信息的真实性、完整性和保密性。但 SSL 不对应用层的消息进行数字签名，因此不能提供交易的不可抵赖性，这是 SSL 在电子商务中使用的最大不足。因此，网景公司在从 Communicator 4.04 版开始的所有浏览器中引入了一种被称做表单签名（Form Signing）的功能。在电子商务中，可利用这一功能对包含购买者的订购信息和付款指令的表单进行数字签名，从而保证交易信息的不可否认性。SSL 协议是一个保证任何安装了安全套接层的客户机和服务器间事务安全的协议，它涉及所有 TCP/IP 应用程序。

(1) SSL 安全协议主要提供 3 方面的服务

① 对用户和服务器进行认证，确保数据发送到正确的客户机和服务器。

② 加密数据以防止数据在传输过程中被窃取。

③ 维护数据的完整性，确保数据在传输过程中不被改变。

(2) SSL 协议的工作流程

服务器认证阶段：①客户端(即消费者)向服务器(即商家)发送一个开始信息 Hello，以便开始一个新的会话连接；②服务器根据客户端的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户端发送的 Hello 信息时将包含生成主密钥所需的信息；③客户端根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；④服务器收到该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

客户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回数字签名后的提问和其公开密钥，从而向服务器提供认证。

从 SSL 协议所提供的服务及其工作流程中可以看出，SSL 协议运行的基础是商家对消费者信息保密的承诺，这有利于商家而不利于消费者。在电子商务初级阶段，能运作电子商务的企业大多是信誉较高的大公司，因此这个问题还没有充分暴露出来。随着电子商务的发展，越来越多的中小型公司也参与了电子商务。在电子支付过程中，中小型公司没有强制的监督机制，这种只有商家对消费者的认证而没有消费者对商家的认证的单一认证问题就越来越突出。虽然在 SSL3.0 中通过数字签名和数字证书可实现浏览器和 Web 服务器双方的身份验证，但是 SSL 协议仍存在一些问题，例如，SSL 协议只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL 协议并不能协调各方间的安全传输和信任关系。在这种情况下，Visa 和 MasterCard 两大信用卡公司组织制定了 SET 协议，为网上信用卡支付提供了全球性的标准。

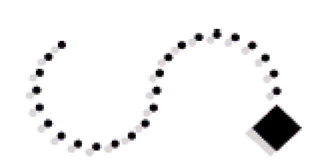
2. SET 协议

SET(Secure Electronic Transcation，安全电子交易)协议由美国 Visa 和 MasterCard 两大信用卡组织联合国际上多家科技机构，共同制定了应用于因特网上的以银行卡为基础进行在线交易的安全标准，目的是保证网络交易的安全。SET 协议主要是为了解决信用卡在电子商务交易中的交易协议、信息保密、资料完整以及身份认证等问题。

SET 协议采用公钥密码体制和 X.509 数字证书标准，主要应用于企业—消费者模式中，保障网上购物信息的安全性。SET 协议本身比较复杂，设计比较严格，安全性高，能保证信息传输的机密性、真实性、完整性和不可抵赖性。SET 协议是公钥基础设施(PKI)框架下的一个典型实现，同时也在不断升级和完善，如 SET2.0 支持借记卡电子交易。

SET 协议的工作流程：

(1) 消费者利用自己的 PC 机通过因特网选定所要购买的物品，并在计算机上输入订货单，订货单上需包括在线商店、购买物品名称及数量、交货时间及地点等相关信息。



（2）通过电子商务服务器与有关在线商店联系，在线商店作出应答，告诉消费者所填订货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。

（3）消费者选择付款方式，确认订单，签发付款指令。此时 SET 开始介入。

（4）在 SET 中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术保证商家看不到消费者的账号信息。

（5）在线商店接受订单后，向消费者所在银行请求支付认可。信息通过支付网关到收单银行，再到电子货币发行公司确认。批准交易后，返回确认信息给在线商店。

（6）在线商店发送订单确认信息给消费者。消费者端软件可记录交易日志，以备将来查询。

（7）在线商店发送货物或提供服务并通知收单银行将钱从消费者的账号转移到商店账号，或通知发卡银行请求支付。在认证操作和支付操作中间一般会有一个时间间隔，例如，在每天的下班前请求银行结一天的账。

SET 从第(3)步开始起作用，一直到第(6)步，在处理过程中，通信协议、请求信息的格式、数据类型的定义等 SET 都有明确的规定。在操作的每一步，消费者、在线商店、支付网关都通过 CA（认证中心）来验证通信主体的身份，以确保通信的对方不是冒名顶替。所以，也可以简单地认为 SET 协议充分发挥了认证中心的作用，以维护在任何开放网络上的电子商务参与者所提供信息的真实性和保密性。

由于 SET 协议提供了消费者、商家和银行之间的认证，确保了交易数据的安全性、完整性、可靠性和交易的不可抵赖性，特别是保证不将消费者银行卡号暴露给商家，因此 SET 协议成为目前公认的信用卡/借记卡的网上交易的国际安全标准。

3. SET 与 SSL 协议的比较

（1）在认证要求方面，早期的 SSL 并没有提供商家身份认证机制，虽然在 SSL3.0 中可以通过数字签名和数字证书实现浏览器和 Web 服务器双方的身份验证，但仍不能实现多方认证；相比之下，SET 的安全要求较高，所有参与 SET 交易的成员（持卡人、商家、发卡行、收单行和支付网关）都必须申请数字证书进行身份识别。

（2）在安全性方面，SET 协议规范了整个电子商务活动的流程，从持卡人到商家，到支付网关，到认证中心以及信用卡结算中心之间的信息流走向和必须采用的加密、认证都制定了严密的标准，从而最大限度地保证了商务性、服务性、协调性和集成性。而 SSL 只对持卡人与商店端的信息交换进行加密保护，SSL 可以看作是用于传输部分的技术规范。从电子商务特性来看，SSL 并不具备商务性、服务性、协调性和集成性。因此 SET 的安全性比 SSL 高。

（3）在网络层协议位置方面，SSL 是基于传输层的通用安全协议，而 SET 位于应用层，对网络上其他各层也有涉及。

（4）在应用领域方面，SSL 主要是和 Web 应用一起工作，而 SET 是为信用卡交易提供安全，因此如果电子商务应用只是通过 Web 或电子邮件，则可以不要 SET。但如果电子商务应用是一个涉及多方交易的过程，则使用 SET 更安全、更通用。

SSL 协议实现简单，独立于应用层协议，大部分内置于浏览器和 Web 服务器中，在电子交易中应用便利。但 SSL 是一个面向连接的协议，只能提供交易中客户与服务器

 间的双方认证，不能实现多方的电子交易。SET在保留对客户信用卡认证的前提下增加了对商家身份的认证，安全性进一步提高。由于两协议所处的网络层次不同，为电子商务提供的服务也不相同，因此在实践中应根据具体情况来选择独立使用或两者混合使用。

4.5 实训：数字证书的申请与应用

1. 数字证书的基本概念

数字证书是用电子手段来证实用户的身份及用户对网络资源的访问权限。数字证书包含用户身份信息、用户公钥信息以及证书发行机构对该证书的数字签名信息。数字证书是利用电子信息技术手段，确认、鉴定、认证因特网上信息交流参与者的身份或服务器的身份，是一个用来担保个人、计算机系统或者组织的身份，并且发布加密算法类别、公开密钥及其所有权的电子文档。

数字证书可用于发送电子邮件、访问站点、网上证券交易、网上购物、网上办公、网上银行和网上签约等安全电子事务处理和安全电子交易活动。

数字证书由数字认证中心(Certificate Authority，CA)发行，该机构负责在发行数字证书之前，证实个人或组织身份和密钥所有权。一般情况下，证书要由社会上公认的、公正的、第三方的可靠组织发行。数字证书要通过CA中心来验证真伪，并逐级往上验证各级认证机构数字证书的真伪。各级认证机构是按根认证机构(Root CA)、品牌认证机构(Brand CA)以及持卡人、商户或收单银行支付风头认证机构由上而下按层次结构建立的。

2. 申请数字证书

目前，世界上已经建立了许多CA认证中心，这些CA的规模、用户数量、技术实力、社会信赖度等存在着差别。中国近年来的电子商务发展较快，各银行的网络银行服务也随之发展起来，信用卡网络支付、网络银行、网上转账等业务已被越来越多的客户接受和应用；同时越来越多的CA认证中心也在中国建立起来，为中国电子商务与金融信息化的发展提供服务。下面以中国数字认证网申请免费数字证书为例，介绍数字证书的申请过程。

中国数字认证网能提供数字认证服务，可用于安全电子邮件、服务器身份认证、客户身份认证、代码签名等服务。中国数字认证网的网站地址为http://www.ca365.com，中国数字认证网界面如图4-8所示。

(1) 安装根证书

① 访问中国数字认证网主页时，如果客户端没有安装根证书，系统会提示用户自动安装根证书，用户一定要按照系统提示选择正确的安装。如果不能自动安装根证书可以手动安装根证书。在中国数字认证网主页的“免费证书”中单击“根CA证书”，弹出“文件下载—安全警告”对话框中单击，如图4-9所示。

② 鼠标单击“打开”按钮，弹出“证书”对话框，如图4-10所示。

③ 单击“安装证书”按钮，弹出“证书导入向导”对话框，如图4-11所示。

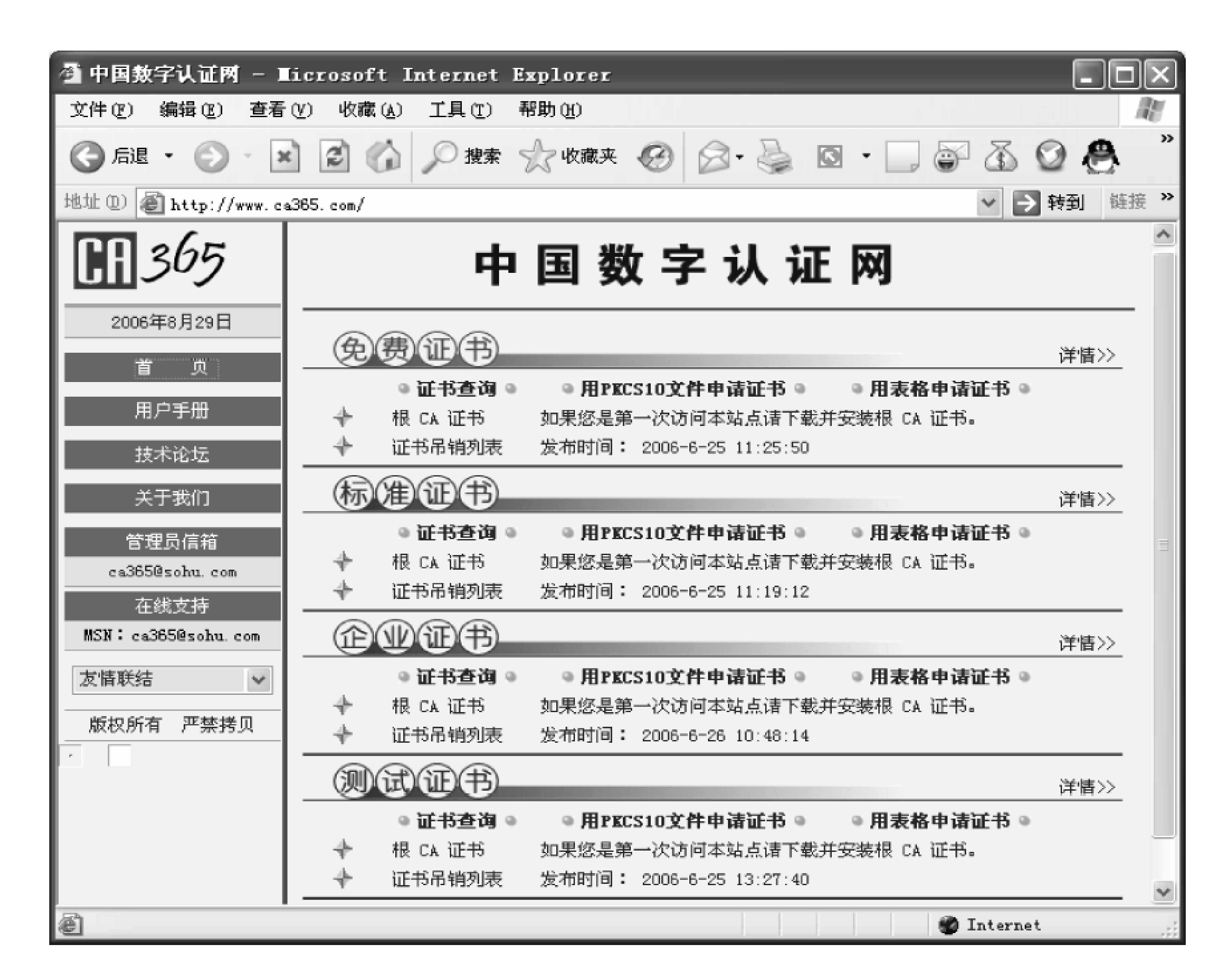


图 4-8　中国数字认证网界面



图 4-9　安装根证书



图 4-10　根证书信息

④ 单击“下一步”按钮，弹出“证书导入向导”对话框，如图 4-12 所示。

⑤ 单击“完成”按钮，弹出“安全警告”对话框，如图 4-13 所示。

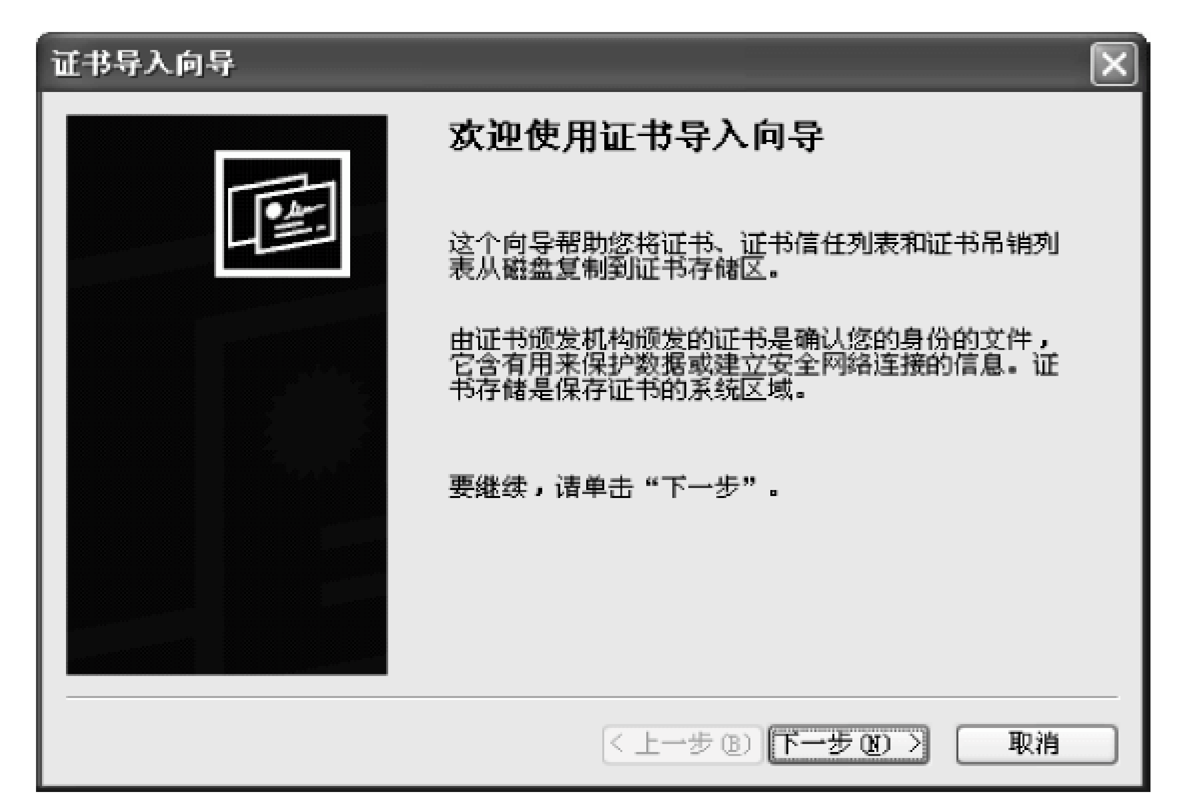


图 4-11 “证书导入向导”对话框



图 4-12 “证书导入向导”对话框



图 4-13 “安全警告”对话框

⑥ 单击“是”按钮，弹出提示框，如图 4-14 所示。

⑦ 单击“确认”按钮，根证书成功安装。

⑧ 打开浏览器窗口，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框的“内容”选项卡，单击“证书”按钮，弹出“证书”对话框，打开“受信任的根证书颁发机构”选项卡，列表中应该有



图 4-14 成功提示框

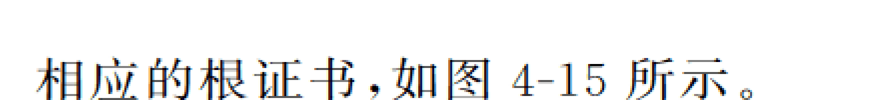

相应的根证书，如图 4-15 所示。



图 4-15　系统中所有证书列表

（2）申请免费证书

① 在中国数字认证网主页的“免费证书”中单击“用表格申请证书”，在如图 4-16 所示的页面中输入证书的信息，在“电子邮件”文本框中一定要输入准备为电子邮件签名的



图 4-16　输入申请人注册信息

电子邮件地址。在“证书用途”下拉列表框中根据证书使用的目的来选择证书用途，在这里选择“电子邮件保护证书”。

② 单击“提交”按钮，弹出“潜在的脚本冲突”对话框，如图 4-17 所示。

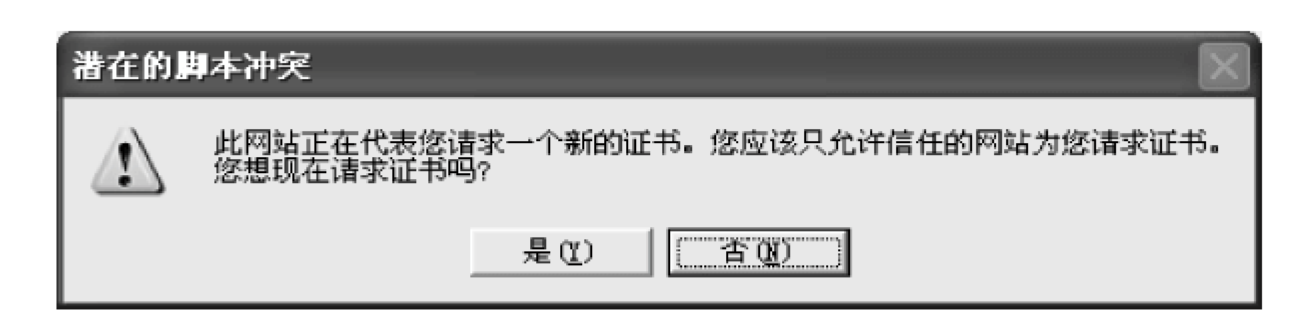


图 4-17　确认申请证书

③ 单击“是”按钮，弹出“正在创建新的 RSA 交换密钥”对话框，如图 4-18 所示。

④ 单击“确定”按钮，成功生成个人电子邮件保护证书。证书成功申请后系统会返回用户的证书序列号如图 4-19 所示，下载证书时需要提供证书的序列号。



图 4-18　“正在创建新的 RSA 交换密钥”对话框

⑤ 在“证书”对话框的“详细信息”选项卡里可以看到证书的序列号，如图 4-20 所示，单击“保存”按钮将证书保存到磁盘，如图 4-17、图 4-18 所示。在“资源管理器”窗口中双击证书文件，也可以打开“证书”对话框。

⑥ 如果证书下载后成功安装，打开浏览器窗口，选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框的“内容”选项卡，单击“证书”按钮，在弹出的“证书”对话框的列表中应该有相应的根证书，如图 4-21 所示。



图 4-19　成功生成个人电子邮件保护证书



图 4-20　个人证书信息



图 4-21　系统已经导入的证书列表

（3）使用个人数字证书

① 在“证书”对话框中选择所要证书，单击“导出”按钮，弹出“证书导出向导”对话框，如图 4-22 所示。

私钥为用户个人所有，不能泄露给其他人，否则别人可以用该私钥以您的名义签名。如果是为了保留证书备份而复制证书，选择“是，导出私钥”单选按钮。如果是为了让其他人为给自己发送加密邮件或有其他用途，不要导出私钥，选择“不，不要导出私钥”单选按钮。如果在申请证书网页中没有选择“标记密钥为可导出”复选框，则不能导出私钥。

② 单击“下一步”按钮，在如图如 4-23 所示的对话框中输入私钥保护密码。如果在申请证书网页中没有选择“启用严格密钥保护”复选框，则没有密码提示。



图 4-22　导出私钥和证书



图 4-23　输入密码保护

③ 单击“下一步”按钮，在弹出的对话框的“文件名”文本框中输入用户想保存的个人数字证书的文件名，或单击“浏览”按钮在弹出的对话框中选择想要保存的目录，按提示进行操作，如图 4-24 所示。

(4) 用个人数字证书完成 Outlook Express 发送签名邮件

发送签名邮件前必须正确安装了自己的电子邮件保护证书(要使用的电子邮件必须与申请证书时填写的电子邮件一致)。

① 在 Outlook Express“工具”菜单中选择“账户”命令,打开“Internet 账户”对话框。

② 选择账户,单击“属性”按钮。在该账户属性对话框的“安全”选项卡中单击“签署证书”选项组中的“选择”按钮,如图 4-25 所示。



图 4-24 保存导出证书

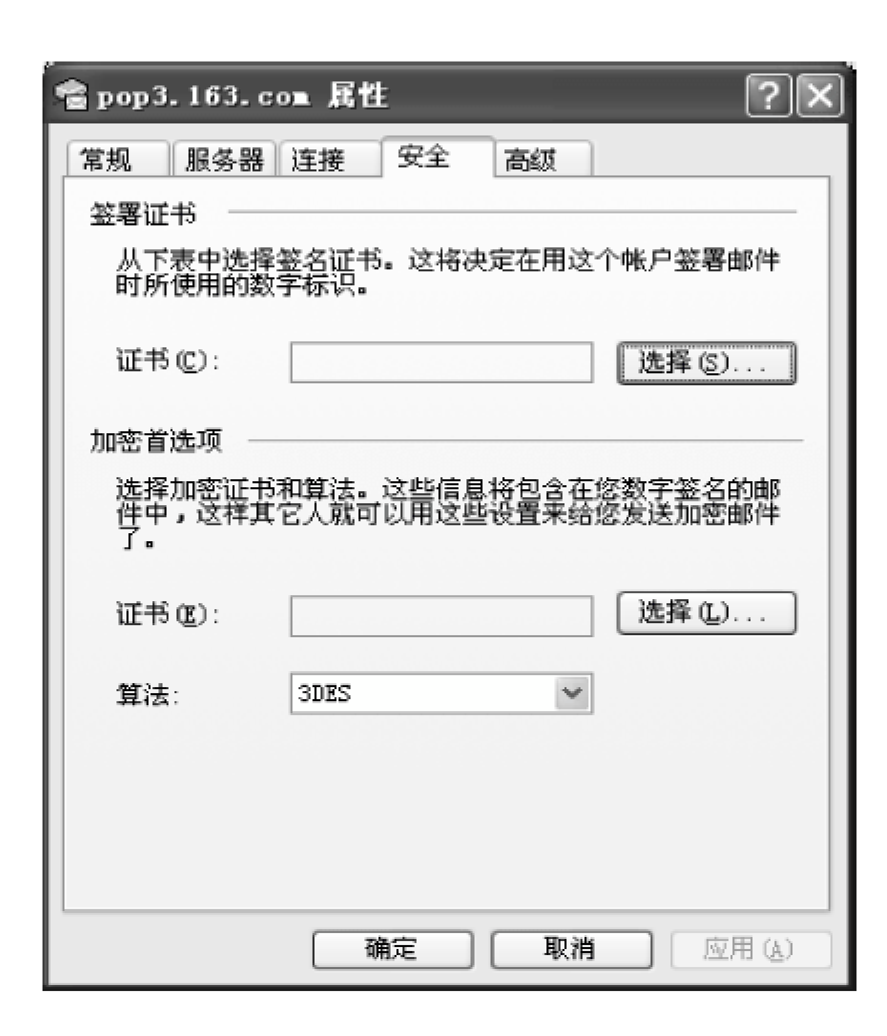


图 4-25 在 Outlook Express 中签署证书

③ 选择证书,单击“确定”按钮,如图 4-26 所示。

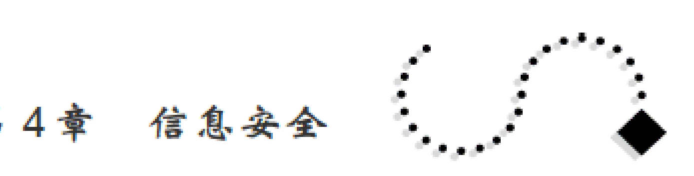
发送邮件时在“新邮件”窗口的“工具”菜单中选择“数字签名”命令,“收件人”文本框后面出现“签名”标志。在该文本框中输入对方邮件地址及其他信息,单击“发送”按钮发送邮件,如图 4-27 所示。



图 4-26 导入要签名的证书



图 4-27 发送新邮件签名



4.6　本章小结

密码技术是信息安全的核心技术，本章介绍了加密算法、密钥管理、数字签名及报文鉴别等常用技术。通过密码技术可以加强网络中传输数据的安全，从而提高网络的安全。本章要求掌握加密算法的种类、密钥分配与管理方法及数字签名的实现过程等内容，对于密码技术在电子商务中的应用要求了解即可。

4.7　本章习题

1. 简述对称性加密和非对称性加密的主要特点。
2. 简述数字签名的实现思想。
3. 简述报文摘要的主要原理。
4. 到相关网站申请数字证书，并在电子邮件中加以应用。

第 5 章

系统安全

【本章内容】

本章主要学习加强计算机网络系统安全的基本方法及常用的技术手段，Kerberos认证、访问控制、防火墙技术 、防计算机病毒技术及黑客的攻防技术等。希望通过学习为进一步的应用打下良好的基础。

【本章重点】

① 熟悉 Windows 2003 在域模式下加强系统安全性的主要方法。

② 掌握计算机病毒的工作过程及常用的反病毒技术。

③ 掌握防火墙的工作原理及体系结构。

④ 了解黑客的攻击过程及常用攻击方法。

加强计算机网络系统的安全性，除了加强计算机网络中传输的数据的安全性之外，还要加强计算机网络中的软件和硬件的安全性。可以从网络体系结构的角度对各层协议的安全性进行加强；也可以从系统运行软件的角度对各种软件的安全性进行加强；还可以针对常见的破坏活动，进行安全的防范等。在本章中仅介绍一些常用的基本技术，即Windows 2003 操作系统提高安全性的主要方法、防火墙技术、防计算机病毒技术及黑客的进攻。

5.1 Windows 2003 操作系统的安全性

操作系统是计算机网络系统配置的最重要的软件，在整个计算机系统中处于中心地位。操作系统的安全与否，是整个计算机网络系统安全性的决定因素之一。下面就介绍Windows 2003 在域工作模式下提高安全性的主要技术。

5.1.1 Kerberos 身份认证

当网络用户对计算机网络中的资源进行访问时，系统首先进行的就是身份认证，只有被认定为合法的客户才有可能进行资源的访问。Windows 2003 在域模式下采用了

Kerberos 身份认证,保证一次登录便可进行全部访问。下面进行简单的介绍。

Kerberos 为网络通信提供可信的面向开放系统的认证服务。当用户(client)申请得到某服务程序(server)的服务时,用户和服务程序会首先向 Kerberos 要求认证对方的身份,认证建立在用户和服务程序对 Kerberos 的信任的基础上。在申请认证时,client 和 server 都可看成是 Kerberos 认证服务的用户,认证双方与 Kerberos 的关系如图 5-1 所示。

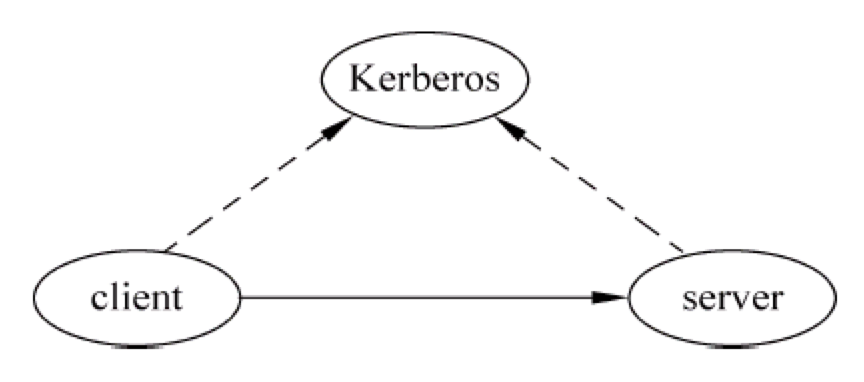


图 5-1　身份验证关系图

当用户登录到工作站时,Kerberos 对用户进行初始认证,通过认证的用户可以在整个登录时间内得到相应的服务。Kerberos 既不依赖用户登录的终端,也不依赖用户所请求的服务的安全机制,而是由 Kerberos 本身提供的认证服务器来完成用户的认证工作。

下面介绍一下 Kerberos 认证的过程。Kerberos 的一些常用术语的简写如表 5-1 所示。

表 5-1　常用术语缩写

简　写	实 际 意 义	简　写	实 际 意 义
c	用户(client)	Kx	x 的私有密钥
s	服务程序(server)	Kx,y	x 和 y 的会话密钥
addr	用户的网络地址	{abc}Kx	用 Kx 加密 abc
ticket	令牌,用于声明用户有效性	Tx,y	x 请求使用 y 的 ticket
life	ticket 保持有效的时间	Ax	x 的标识符(authenticator)
tgs,TGS	票证服务器	WS	工作站
AS	认证服务程序		

Kerberos 有两种证书(crendentials):ticket 和 authenticator。这两种证书均使用密钥加密,但加密的密钥不同。

ticket 用来在认证服务器和用户请求的服务之间传递用户的身份,同时也传递附加信息来保证使用 ticket 的用户必须是 ticket 中指定的用户。ticket 的组成部分,如图 5-2 所示。

```
Tc,s={s,c,addr,timestamp,life,Ks,c}Ks;
```

图 5-2　令牌构成

ticket 由 client 和 server 的名字、client 的地址、时间戳、生存时间、会话密钥 5 部分组成。ticket 一旦生成,在 life 指定的时间内可以被 client 多次使用来申请同一个 server 的服务。

authenticator 则提供信息与 ticket 中的信息进行比较,保证发出 ticket 的用户就是 ticket 中指定的用户。authenticator 的组成部分,如图 5-3 所示。

```
Ac={c,addr,timestamp}Ks,c;
```

图 5-3　标识符的构成

authenticator 由 client 的名字、client 的地址、记录当前时间的时间戳 3 部分组成。authenticator 只能在一次服务请求中使用，每当 client 向 server 申请服务时，必须重新生成 authenticator。

用户 c 请求服务 s 的整个 Kerberos 认证协议如图 5-4 所示。

（1）用户 c 得到初始化令牌 Tc，tgs

登录时用户输入用户名后，系统会向认证服务器（authentication server）发送一条包含用户和 tgs（ticket granting server）服务两者名字的请求。认证服务器检查用户是否有效，如果有效，则随机产生一个用户用来和 tgs 通信的会话密钥 Kc，tgs，然后创建一个令牌 Tc，tgs，令牌中包含用户名、tgs 服务名、用户地址、当前时间、有效时间，还有刚才创建的会话密钥，然后将令牌用 Ktgs 加密。认证服务器向用户发送加密过的令牌{Tc，tgs}Ktgs 和会话密钥 Kc，tgs，发送的消息用只有用户和认证服务器知道的 Kc 来加密，Kc 的值基于用户的密码，用户与 AS 之间的数据交换，如图 5-5 所示。



图 5-4　Kerberos 认证协议图　　　图 5-5　用户与 AS 之间的数据交换

用户工作站收到认证服务器回应后，就会要求用户输入密码，将密码转化为 DES 密钥 Kc，然后将认证服务器发回的信息解开，将令牌和会话密钥保存用于以后的通信，为了安全，用户密码和密钥 Kc 则被删掉。

当用户的登录时间超过了令牌的有效时间时，用户的请求就会失败，这时系统会要求用户通过 kinit 程序重新申请令牌 Tc，tgs。用户运行 klist 命令可以查看自己所拥有的令牌的当前状态。

（2）用户 c 从 tgs 得到所请求服务 s 的令牌 Tc，s

一个令牌只能申请一个特定的服务，所以用户必须为每一个服务 s 申请新的令牌，用户可以从 tgs 处得到令牌 Tc，s。

用户程序首先向 tgs 发出申请令牌的请求，请求信息中包含 s 的名字、得到的请求 tgs 服务的加密令牌{Tc，tgs}Ktgs，还有加密过的 Authenticator 信息{Ac}Kc，tgs，Kc，tgs 就是第（1）步得到的会话密钥。

tgs 得到请求后，用密钥和会话密钥解开请求得到 Tc，tgs 和 Ac，根据两者的信息鉴定用户身份是否有效。如果有效，tgs 生成用于 c 和 s 之间通信的会话密钥 Kc，s，并生成用于 c 申请得到 s 服务的令牌 Tc，s，其中包含 c 和 s 的名字、c 的网络地址、当前时间、有效时间和刚才产生的会话密钥。令牌 Tc，s 的有效时间是初始令牌 Tc，tgs 剩余的有效时间和所申请的服务默认有效时间中最短的时间。用户与 tgs 之间的数据交换，如图 5-6 所示。

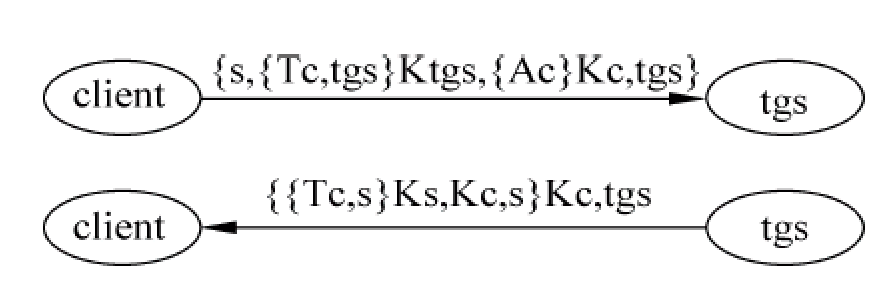
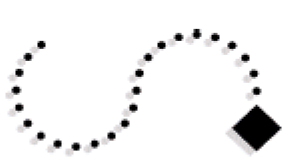


图 5-6　用户与 tgs 之间的数据交换

tgs 最后将加密后的令牌{Tc，s}Ks 和会话



密钥 Kc,s 用用户和 tgs 之间的会话密钥加密后发送给用户。用户 c 得到回答后,用 Kc,tgs 解密,得到所请求的令牌和会话密钥。

(3) 用户 c 利用得到的令牌 Kc,s 申请服务 s。用户申请服务 s 的工作与第(2)步相似,只不过申请的服务由 tgs 变为 s。

用户首先向 s 发送包含加密令牌{Tc,s}Ks 和{Ac}Kc,s 的请求,s 收到请求后将其分别解密,并比较得到的用户名、网络地址、时间等信息,判断请求是否有效。用户和服务程序之间的时钟必须同步在几分钟的时间段内,当请求的时间与系统当前时间相差太远时,认为该请求是无效的,以免遭到重放攻击。为了防止重放攻击,s 通常保存一份最近收到的有效请求的列表,当收到一份请求与已经收到的某份请求的令牌和时间完全相同时,认为此请求无效。

当 c 也想验证 s 的身份时,s 将收到的时间戳加 1,并用会话密钥加密后发送给用户,用户收到回答后,用会话密钥解密来确定 s 的身份,服务器与客户机之间的数据交换,如图 5-7 所示。

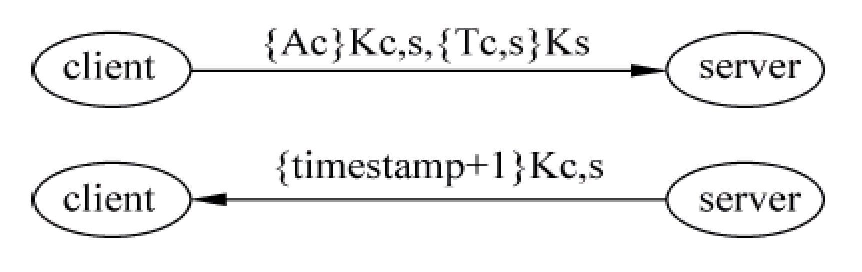


图 5-7　服务器与客户机之间的数据交换

通过上面 3 步之后,用户 c 和服务 s 互相验证了彼此的身份,并且拥有只有 c 和 s 两者知道的会话密钥 Kc,s,c 和 s 以后的通信都可以通过该会话密钥得到保护。

5.1.2　访问控制

当用户成功登录到系统后,用户就领到了一张身份证件,而系统中各种资源都包含控制用户访问的控制信息。当用户访问资源时,系统将对比资源的访问控制信息和用户的身份证件,以确定用户是否有权访问资源,以及访问权限是什么。

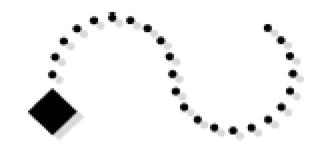
1. 安全标识符 SID(Security Identifier)

SID 是标识用户、组和计算机账户的惟一的号码。在第一次创建该账户时,将给网络上的每一个账户发布一个惟一的 SID。Windows 2003 中的内部进程将引用账户的 SID 而不是账户的用户名或组名。如果先创建账户,再删除账户,然后使用相同的用户名创建另一个账户,则新账户将不具有授权给前一个账户的权力或权限,原因是该账户具有不同的 SID 号。安全标识符也被称为安全 ID 或 SID。

用户通过验证后,登录进程会给用户一个访问令牌,该令牌相当于用户访问系统资源的票证。当用户访问系统资源时,将访问令牌提供给 Windows,然后 Windows 检查用户访问对象上的访问控制列表。如果用户被允许访问该对象,Windows 将会分配给用户适当的访问权限。

访问令牌是用户在通过验证的时候由登录进程提供的,所以改变用户的权限需要注销后重新登录,重新获取访问令牌。

如果存在两个同样 SID 的用户,这两个账户将被鉴别为同一个账户。如果账户无限制增加的时候,系统可能会产生同样的 SID,在通常的情况下 SID 是惟一的。SID 由计算机名、当前时间、当前用户状态线程的 CPU 耗费时间的总和 3 个参数决定,以保证 SID 的惟一性。



一个完整的 SID 包括：用户和组的安全描述、48 位的 ID 标识、修订版本、可变的验证值，例如，s-1-5-21-76985614-1876338704-322544478-1001。

2. 访问控制

既然用户登录到服务器上，就可以对照基于 NTFS 文件系统的任意访问控制列表(DACL)查找用户的权限。当一个用户试图访问一个文件或者文件夹的时候，NTFS 文件系统会检查用户使用的账户或者账户所属的组是否在此文件或者文件夹的访问控制列表(ACL)中，如果存在则进一步检查访问控制项(ACE)，然后根据控制项中的权限来判断用户最终的权限。如果访问控制列表中不存在用户使用的账户或者账户所属的组，就拒绝用户访问。

(1) NTFS 权限及对应的操作

NTFS 权限及对应的操作如表 5-2 所示。

表 5-2　NTFS 权限及对应的操作

NTFS 权限	对应的操作
完全控制	对文件或者文件夹可执行所有操作
修改	可以修改、删除文件或者文件夹
读取和运行	可以读取内容，并且可以执行应用程序
列出文件夹目录	可以列出文件夹内容，此权限只针对文件夹存在
读取	可以读取文件或者文件夹的内容
写入	可以创建文件或者文件夹
特别的权限	其他不常用的权限，比如删除权限的权限

NTFS 的所有权限都有“允许”和“拒绝”两种选择，如图 5-8 所示。

关于权限的进一步说明如下：

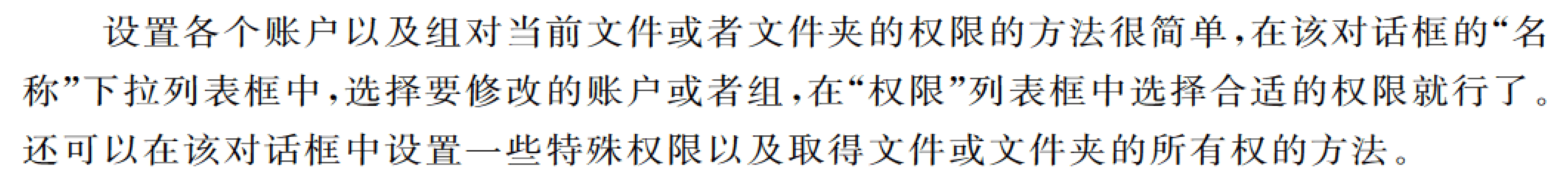
① 新建的文件或者文件夹都有默认的 NTFS 权限，如果没有特别需要，一般不用改。文件或者文件夹的默认权限是继承上一级文件夹的权限，如果是根目录(比如 C：\)下的文件夹，则权限是继承磁盘分区的权限。权限的设置在如图 5-9 所示的对话框中进行。



图 5-8　NTFS 权限及对应的操作



图 5-9　权限的设置



设置各个账户以及组对当前文件或者文件夹的权限的方法很简单，在该对话框的“名称”下拉列表框中，选择要修改的账户或者组，在“权限”列表框中选择合适的权限就行了。还可以在该对话框中设置一些特殊权限以及取得文件或文件夹的所有权的方法。

② NTFS 权限的应用规则。如果一个用户同时在两个组或者多个组内，而各个组对同一个文件有不同的权限，那么这个用户对这个文件有什么权限呢？

简单地说，当一个用户属于多个组的时候，这个用户会得到各个组的累加权限，但是如果有一个组的相应权限被拒绝，则用户的此权限也会被拒绝。

举例来说，假设有一个用户 WZ，如果 WZ 属于 A 和 B 两个组，A 组对某文件有读取权限，B 组对此文件有写入权限，WZ 对此文件有修改权限，那么 WZ 对此文件的最终权限为读取＋写入＋修改权限。

假设 WZ 对文件有写入权限，A 组对此文件有读取权限，但是 B 组对此文件为拒绝读取权限，那么 WZ 对此文件只有写入权限。这里还有一个小问题，WZ 对此文件只有写入权限，没有读取权限，那么，写入权限有效么？答案很明显，WZ 对此文件的写入权限无效，因为不能读取怎么写入？连门都进不去，怎么把家具搬进去？

③ 权限的继承。新建的文件或者文件夹会自动继承上一级目录或者驱动器的 NTFS 权限，但是从上一级继承下来的权限是不能直接修改的，只能在此基础上添加其他权限。也就是不能把权限上的勾去掉(因为你去不掉)，只能添加新的勾。在“属性”窗口中灰色的框为继承的权限，是不能直接修改的，白色的框是可以添加的权限。

当然这并不是绝对的，只要权限够，比如管理员，也可以把这个继承下来的权限修改了，或者让文件不再继承上一级目录或者驱动器的 NTFS 权限。

④ 权限的拒绝。这个很简单，只要记住，拒绝的权限是最大的就行了。无论给账户或者组设置了什么权限，只要“拒绝”复选框被选中，那么被拒绝的权限就绝对有效。

⑤ 移动和复制操作对权限的影响。这里一共有 4 种情况，移动或复制文件(夹)到同一或者不同分区内。只需要记住，只有移动到同一分区内才能保留原来设置的权限，否则权限为继承目的地文件夹或者驱动器的 NTFS 权限。

(2) 共享权限

共享权限只有 3 种：读取、更改和完全控制。Windows Server 2003 默认的共享文件设置权限是 Everyone 用户只具有读取权限，如图 5-10 所示。Windows 2000 默认的共享文件设置权限是 Everyone 用户具有完全控制权限。



图 5-10　共享权限

下面解释一下 3 种权限。

• 读取权限是指派给 Everyone 组的默认权限。除此之外 Everyone 组的用户还能进行如下操作：查看文件名和子文件夹名、

查看文件中的数据、运行程序文件。

- 更改权限不是任何组的默认权限。更改权限除允许所有的读取权限外，还增加以下操作：添加文件和子文件夹，更改文件中的数据，删除子文件夹和文件。
- 完全控制权限是指派给本机上的 Administrators 组的默认权限，包括读取及更改权限。

和 NTFS 权限一样，如果赋予某用户或者用户组拒绝的权限，则该用户或者该用户组的成员将不能执行被拒绝的操作。

对于共享文件夹应注意如下 4 点。

① 在 Windows 2000 中，共享的文件夹可以用空密码用户访问，但是在 Windows Server 2003 中，共享的文件夹不可以用空密码用户访问，这是比较常见的网络共享无法访问的问题，希望注意。

② 共享权限只对通过网络访问的用户有效，所以有时需要和 NTFS 权限配合(如果分区是 FAT/FAT32 文件系统，则不需要考虑)，才能严格地控制用户的访问。当一个共享文件夹设置了共享权限和 NTFS 权限后，就要受到两种权限的控制。

③ 如果希望用户能够完全控制共享文件夹，首先要在共享权限中添加此用户(组)，并设置完全控制的权限，然后在 NTFS 权限设置中添加此用户(组)，也设置完全控制权限。只有两个地方都设置了完全控制权限，用户(组)才最终拥有完全控制权限。

④ 当用户从网络访问一个存储在 NTFS 文件系统上的共享文件夹的时候，会受到两种权限的约束，而有效权限是最严格的权限(也就是两种权限的交集)。而当用户从本地计算机直接访问文件夹的时候，不受共享权限的约束，只受 NTFS 权限的约束。同时还要考虑到两个权限的冲突问题，例如，共享权限为只读，NTFS 权限是写入，那么最终权限是完全拒绝，因为这两个权限的组合权限是两个权限的交集。

5.2 防火墙技术

5.2.1 什么是防火墙

防火墙就像中世纪的城堡防卫系统，那时人们为了保护城堡的安全，在城堡的周围挖一条护城河，每一个进入城堡的人都要经过吊桥，并且还要接受城门守卫的检查。人们借鉴了这种防护思想，设计了一种网络安全防护系统，这种系统就被称为防火墙，如图 5-11 所示。

计算机网络中的防火墙技术是建立在现代通信技术和信息安全技术基础上的应用性安全技术，应用于内部网络与外部网络的中间，保障内部网络的安全。防火墙可以在用户的计算机和因特网之间建立一道屏障，把用户和外部网络隔绝；用户可以通过设定规则来决定哪些情况下防火墙应该隔绝计算机与因特网之间的数据传输，哪些情况下允许两者之间的数据传输。通过防火墙挡住外部网络对内部网络的攻击和入侵，从而保障用户的网络安全。

从逻辑上讲，防火墙是分离器、限制器和分析器，有效地控制了内部网络和因特网之

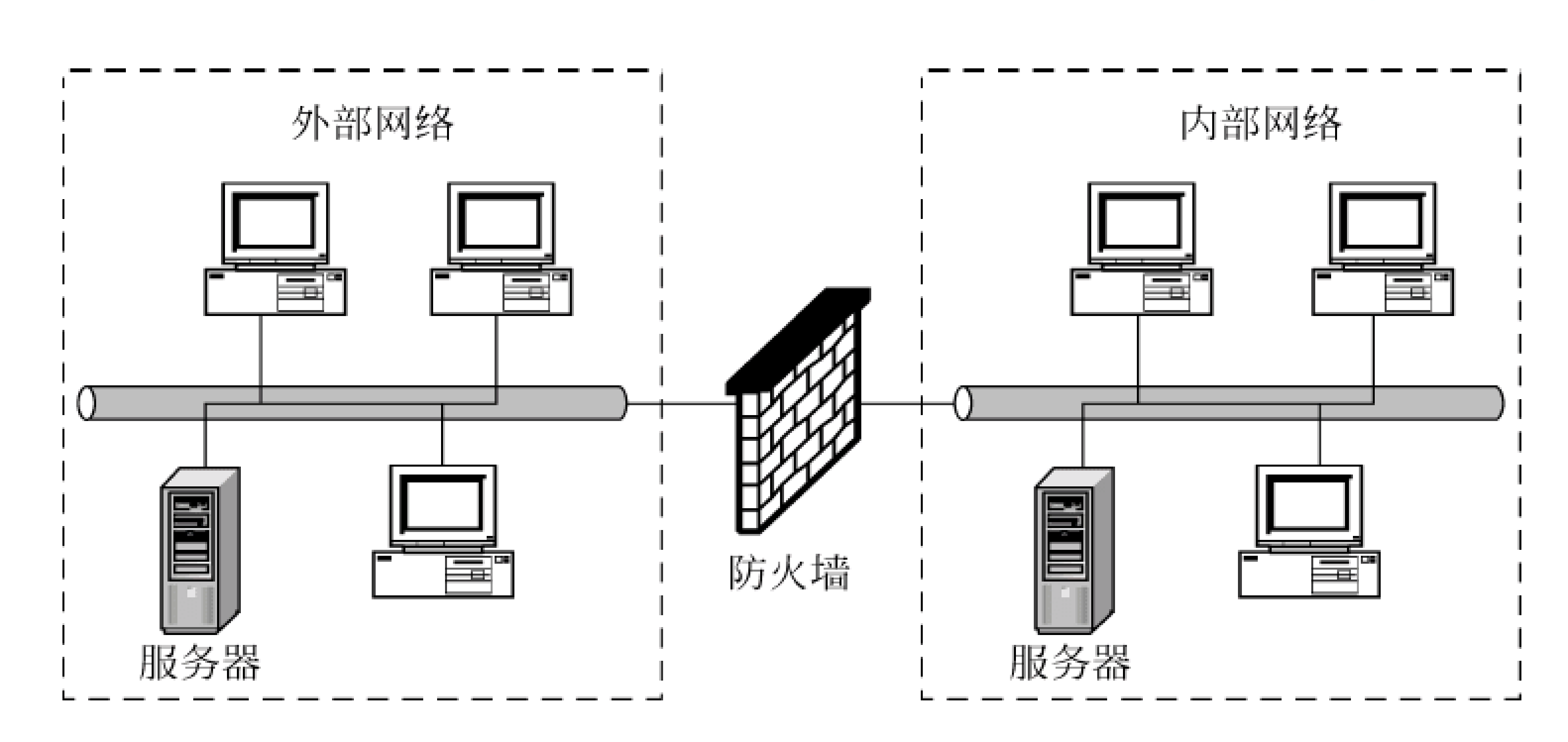


图 5-11　防火墙

间的任何活动，保证了内部网络的安全。在计算机网络中，防火墙是一个活动的屏障，并可通过一个“门”来允许用户在安全网络和开放的不安全的网络之间通信。早期的防火墙是由一个单独的机器组成的，放置在私有网络和公网之间。近些年来，防火墙涉及整个从内部网络到外部网络的区域，由一系列复杂的机器和程序组成。简单地说，今天的防火墙是多个组件的应用。从实现形式上讲，防火墙可以分为硬件防火墙和软件防火墙，硬件防火墙是通过硬件和软件的结合来达到隔离内、外部网络的目的；软件防火墙是通过纯软件的方式来实现的。

防火墙在实施安全的过程中是至关重要的。一个防火墙策略要符合 4 个目标，而每个目标通常都不是通过一个单独的设备或软件来实现的。大多数情况下防火墙的组件放在一起使用以满足公司安全目的的需求。

(1) 实现一个公司的安全策略

防火墙的主要意图是强制执行你的安全策略。在前面的课程提到过在适当的网络安全中安全策略的重要性。举个例子，也许你的安全策略只需对 MAIL 服务器的 SMTP 流量作些限制，那么你要直接在防火墙强制这些策略。

(2) 创建一个阻塞点

防火墙在一个公司私有网络和公网间建立一个检查点，要求所有的流量都要通过这个检查点。一旦这些检查点建立起来，防火墙设备就可以监视、过滤和检查所有进来和出去的流量。网络安全产业称这些检查点为阻塞点。通过强制所有进出流量都通过这些检查点，网络管理员可以集中在较少的地方来进行监测。如果没有这样一个供监视和控制信息的点，系统或安全管理员则要在大量的地方来进行监测。检查点的另一个名字叫做网络边界。

(3) 记录因特网活动

防火墙还能够强制日志记录，并且提供警报功能。通过在防火墙上实现日志服务，安全管理员可以监视所有从外部网或互联网的访问。好的日志策略是实现适当网络安全的有效工具之一。防火墙对于管理员进行日志存档提供了更多的信息。

(4) 限制网络暴露

防火墙在内部网络周围创建了一个保护的边界，并且对于公网隐藏了内部系统的一些信息以增加保密性。当远程节点侦测内部网络时，它们仅仅能看到防火墙。远程设备



 将不会知道内部网络的布局。防火墙可以通过提高认证功能和对网络加密来限制网络信息的暴露。通过对所有进来的流量进行源检查,以限制从外部发动的攻击。

防火墙的缺点主要集中在以下 4 点。

(1) 不能防范恶意的知情者

如果入侵者在防火墙的内部,它不通过防火墙就可以删改文件,盗窃数据,破坏软件和硬件。这种情况下防火墙是无能为力的,只能加强内部管理来防范。

(2) 不能防范不通过它的连接

如果内部网被允许不通过防火墙,而通过其他途径进行访问,那么不通过防火墙的非法访问不能被防范。

(3) 不能防备全部的威胁

防火墙可以用来防范已知的威胁,但不能防范未知的新威胁。

(4) 不能防病毒

虽然防火墙扫描所有通过的信息,但是不能扫描数据的确切内容,即使是先进的数据包过滤也不能防范数据中隐藏的病毒。

5.2.2 防火墙的基本技术

1. 分组过滤技术

分组过滤技术是防火墙应用的最基本的技术,可以用来实现多种网络安全策略。网络安全策略必须明确描述被保护的资源、服务的类型、重要程度以及防范对象。

首先在分组过滤装置的端口设置分组过滤准则(分组过滤规则),分组过滤的规则按一定的顺序存储。当一个分组到达端口时,对分组的头部进行分析,大多数分组过滤装置只检查 IP、传输控制协议(TCP)、用户数据报文协议(UDP)头部内的字段。然后根据分组过滤的规则来决定是阻塞该分组还是继续发送。如果存在某条规则阻塞一个分组传递或接收,则不允许该分组通过。如果存在某条规则允许或接收一个分组,则允许该分组通过。如果一个分组不满足任何规则,则该分组被阻塞。分组过滤原理如图 5-12 所示。

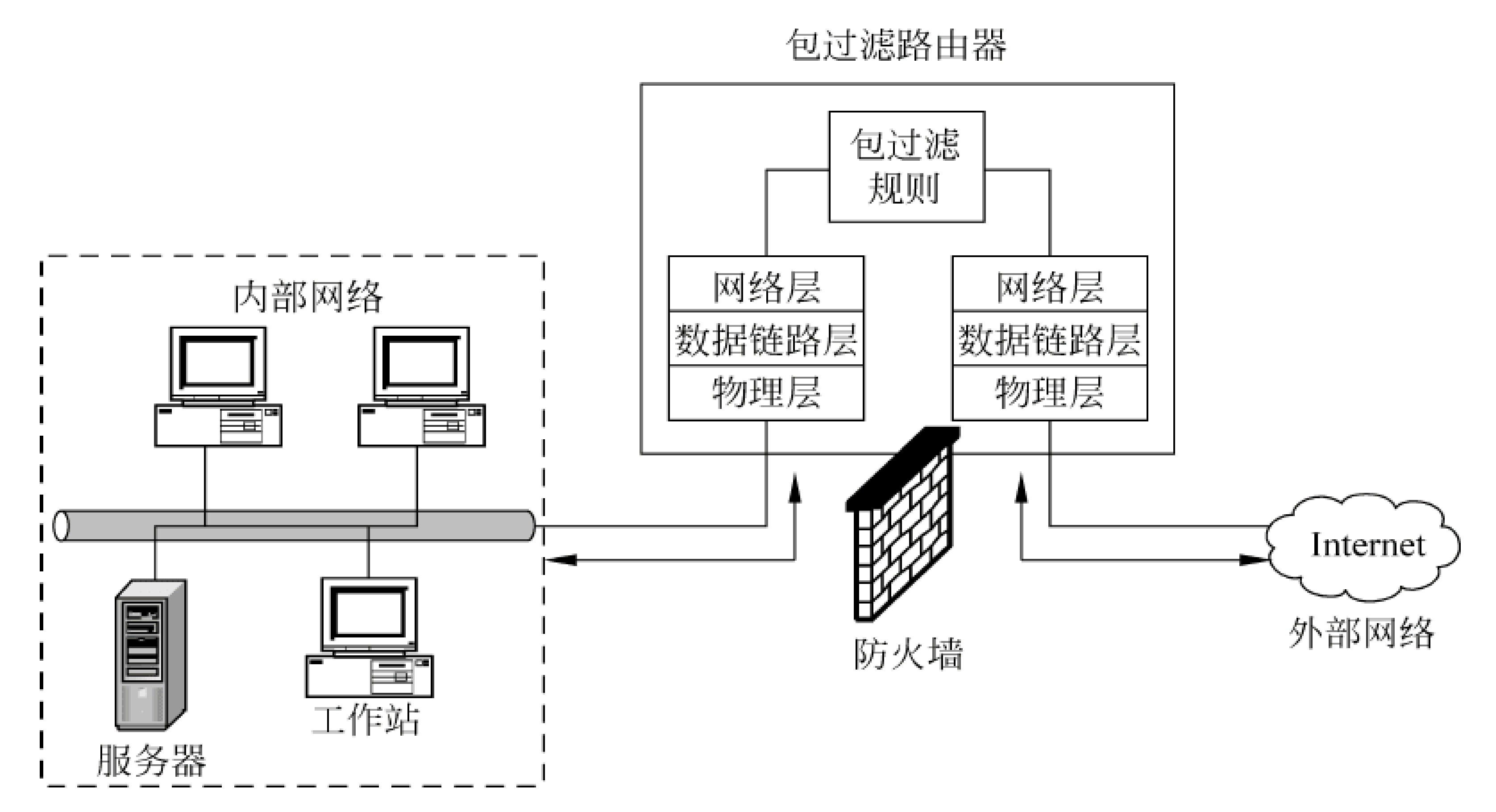
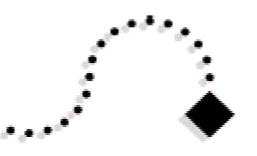


图 5-12 分组过滤原理示意图



下面根据一个简单的例子来说明分组过滤的工作原理。

有一个内部网 A,它的 IP 地址为 132.36.X.X,其中的某部门的 IP 地址为 132.36.9.X。另一个内部网 B 的 IP 地址为 112.44.X.X,其中的某部门 IP 地址为 112.44.9.X,该部门不能连接到 A 的内部网,允许 B 其他部门的所有子网与 A 内部网 132.36.9.X 连接,但不能与 A 其他部门连接。过滤规则表如表 5-3 所示。

表 5-3　过滤规则表

规则	源　地　址	目 的 地 址	动作
1	112.44.X.X	132.36.9.X	允许
2	112.44.9.X	132.36.X.X	拒绝
3	0.0.0.0	0.0.0.0	拒绝

当一个分组到达过滤端口时,分别用过滤规则表中的每条规则对分组进行检查,符合规则 1 的允许通过,符合规则 2 的将被拒绝,不允许通过。表中的规则 3 为默认值,也就是不符合规则 1 和规则 2 的其他分组将被拒绝,不允许通过。

根据规则表可以得到以下结论:

对于分组 1,源地址 112.44.9.1,目的地址 131.36.1.1,则拒绝该分组通过。

对于分组 2,源地址 112.44.1.1,目的地址 131.36.9.1,则允许该分组通过。

对于分组 3,源地址 112.24.1.1,目的地址 131.36.1.1,则拒绝该分组通过。

一个分组过滤装置常被放置于一个或几个网段与其他网段之间。网段通常被分为内部网段和外部网段,外部网段用来连接外部网络,例如,因特网;内部网段用来连接一个单位或组织内部的主机和其他网络资源。

2. 应用代理技术

应用代理实际上是应用程序代理技术,是建立在应用层的基础上,利用应用程序来过滤 Telnet、FTP 等服务连接,这样的应用软件称为代理服务。运行代理服务的主机称为应用网关,代理服务仅允许在应用网关有代理的服务通过防火墙,而其他没有代理的服务将被阻塞。代理服务具有认证和很强的日志功能。

应用程序代理防火墙实际上并不允许在它连接的网络之间直接通信。代理服务器接受来自内部网络特定用户应用程序的通信,然后建立与公共网络服务器单独的连接。网络内部的用户不直接与外部的服务器通信,所以服务器不能直接访问内部网的任何一部分。

另外,如果不为特定的应用程序安装代理程序代码,这种服务是不会被支持的,不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接,从而提供了额外的安全性和控制性。应用代理示意图如图 5-13 所示。

例如,一个用户的 Web 浏览器可能在 80 端口,但也可能是在 1080 端口,连接到了内部网络的 HTTP 代理防火墙。防火墙接受这个连接请求,并把它转到所请求的 Web 服务器。

这种连接和转移对该用户来说是透明的,因为它完全是由代理防火墙自动处理的。代理防火墙通常支持一些常见的应用服务,如 HTTP、HTTPS/SSL、SMTP/POP3、IMAP、NNTP、Telnet、FTP、IRC。

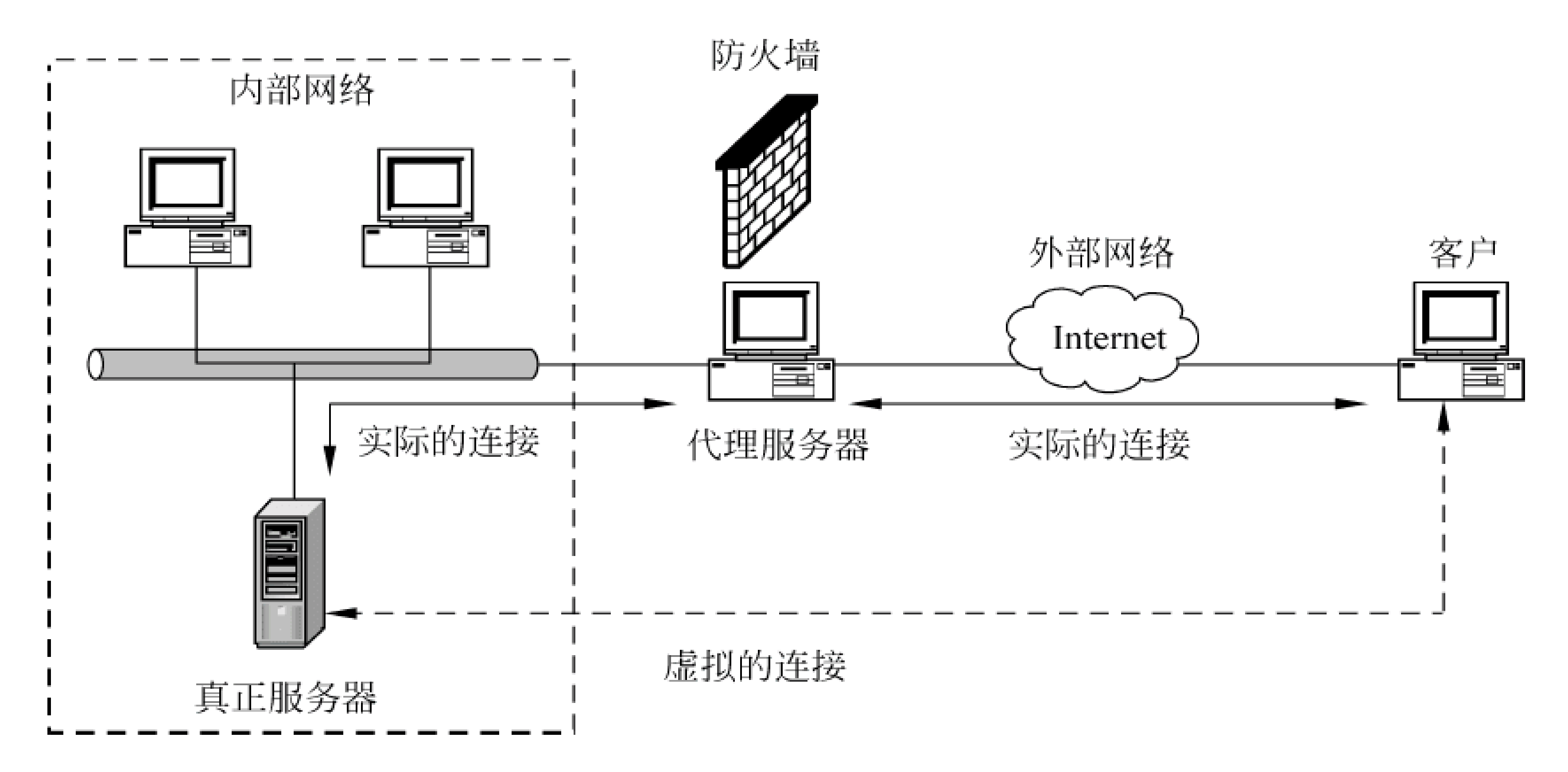


图 5-13　应用代理示意图

应用程序代理防火墙可以配置成允许来自内部网络的任何连接，也可以配置成要求用户认证后才建立连接。要求认证的方式有只为已知的用户建立连接这种限制，为安全性提供了额外的保证。如果网络受到危害，这个功能使得从内部发动攻击的可能性大大减少。

3. 监测模型技术

监测模型技术是根据因特网和内部网络关联的需求，建立其控制管理的模型，完成信息传输的控制与管理。从原理上讲监测模型技术对所有的协议都有效，能处理从 IP 层到应用层所有的分组过滤数据，也就是将所有层的信息综合到一个监测点上进行过滤。一般是加载一个检测模块，在不影响网络正常工作的前提下，检测模块在网络层截取数据包，然后在所有的通信层上抽取有关的状态信息，据此判断该通信是否符合安全策略。由于监测模型技术是在网络层截获数据包的，因此可以支持多种协议和应用程序，并可以很容易地实现应用的扩充。

5.2.3 防火墙的体系结构

最简单的防火墙配置，就是直接在内部网和外部网之间加装一个包过滤路由器或者应用网关。为更好地实现网络安全，有时还要将几种防火墙组合起来构建防火墙系统。目前比较流行的有以下 3 种防火墙配置方案。

1. 双宿主机网关

双宿主机网关是用一台装有两个网络适配器的双宿主机做防火墙。双宿主机用两个网络适配器分别连接两个网络，又称为堡垒主机。堡垒主机上运行着防火墙软件（通常是代理服务器），可以转发应用程序，提供服务等。双宿主机网关有一个致命弱点，一旦入侵者侵入堡垒主机并使该主机只具有路由器功能，则任何网上用户均可以随便访问有保护的内部网络，如图 5-14 所示。

2. 屏蔽主机网关

屏蔽主机网关易于实现，安全性好，应用广泛。屏蔽主机又分为单宿堡垒主机和双宿

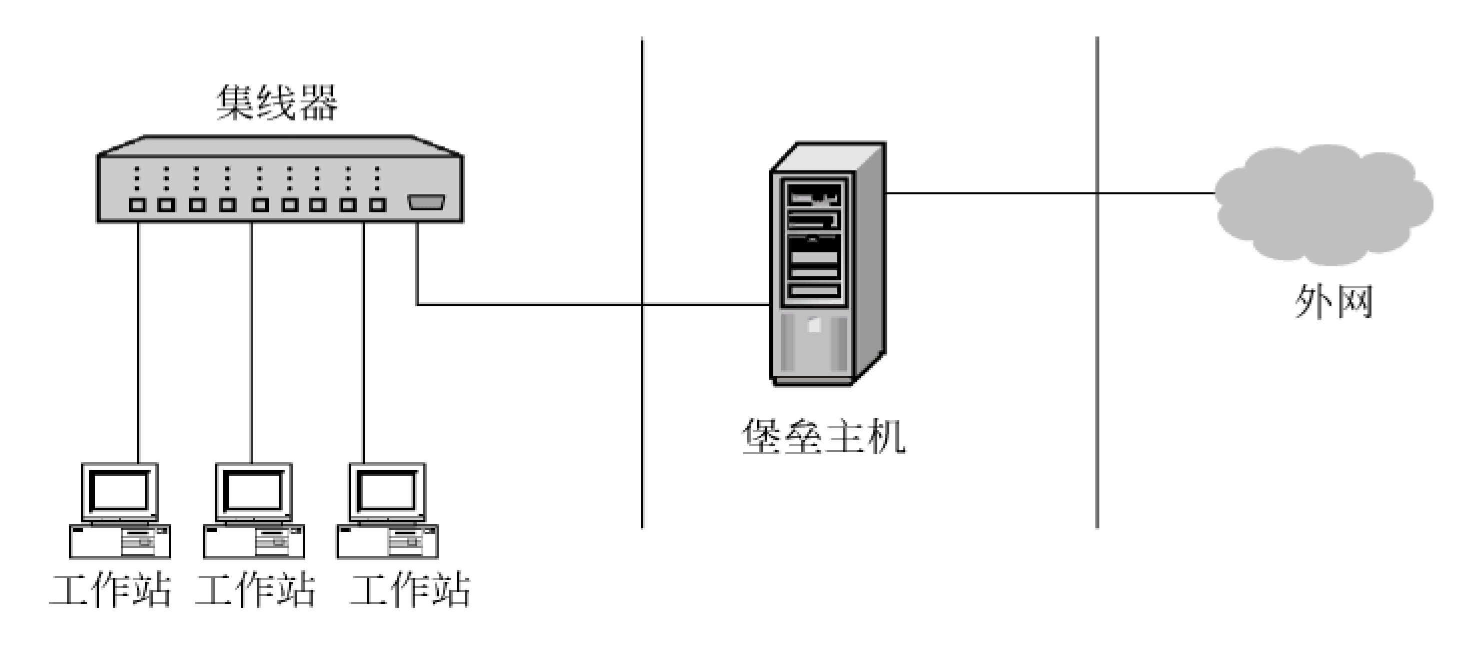


图 5-14　双宿主机网关

堡垒主机两种类型。在单宿堡垒主机类型中，一个包过滤路由器连接外部网络，一个堡垒主机安装在内部网络上。堡垒主机只有一个网卡，与内部网络连接。通常在路由器上设立过滤规则，并使这个单宿堡垒主机成为从因特网上惟一可以访问的主机，确保内部网络不受未被授权的外部用户的攻击。而内联网内部的客户机，可以受限制地通过屏蔽主机和路由器访问因特网。单宿堡垒主机如图 5-15 所示。

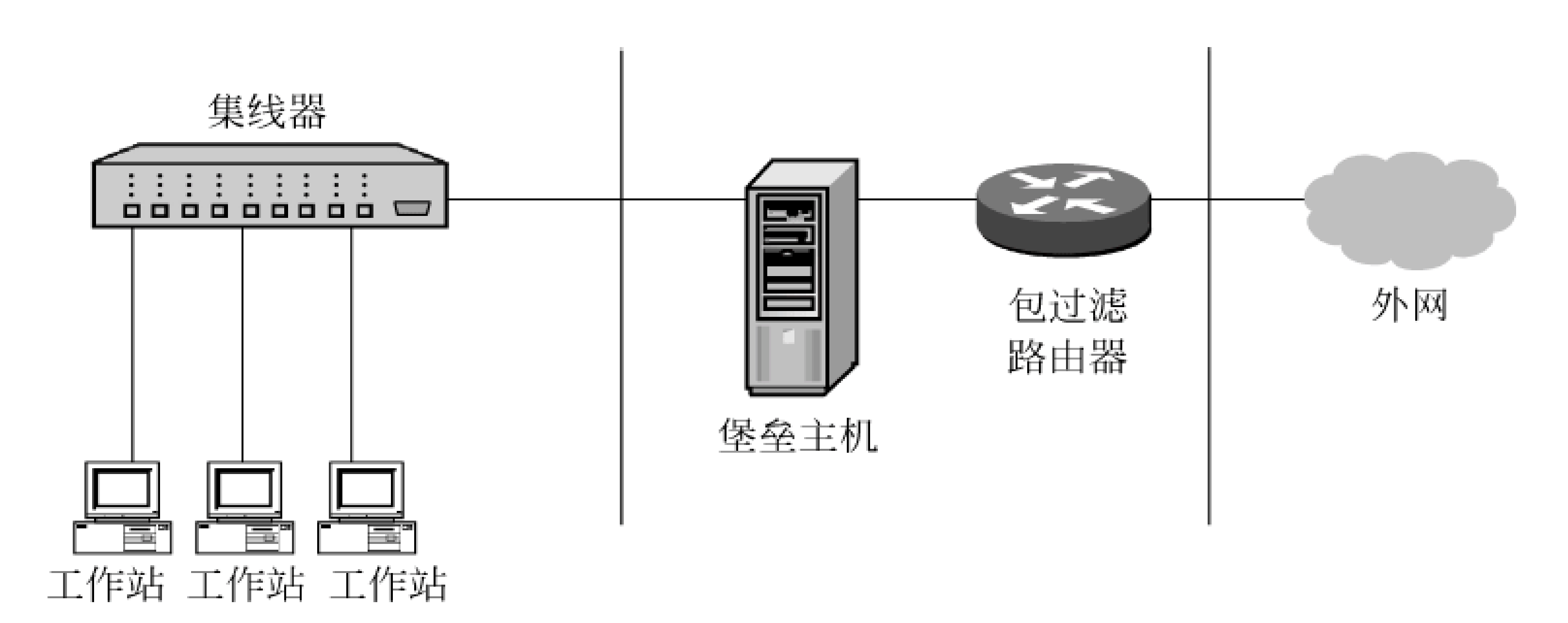


图 5-15　单宿堡垒主机

双宿堡垒主机型与单宿堡垒主机型的区别是，双宿堡垒主机有两块网卡，一块连接内部网络，一块连接包过滤路由器。双宿堡垒主机在应用层提供代理服务，与单宿型相比更加安全。双宿堡垒主机如图 5-16 所示。

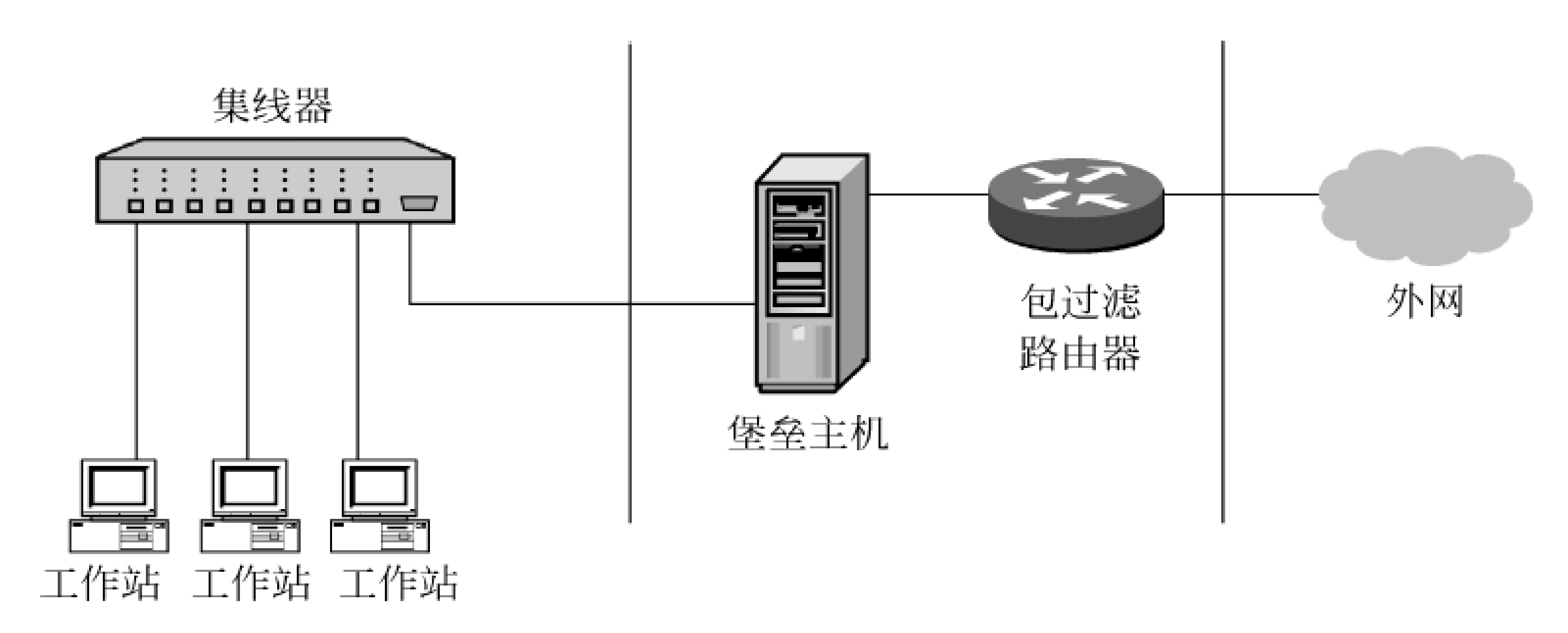


图 5-16　双宿堡垒主机

3. 屏蔽子网

屏蔽子网是在内联网和因特网之间建立一个被隔离的子网，用两个包过滤路由器将这一子网分别与内联网和因特网分开。两个包过滤路由器放在子网的两端，在子网内构成一个“缓冲地带”，两个路由器一个控制内联网数据流，另一个控制因特网数据流，内联网和因特网均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。可根据需要在屏蔽子网中安装堡垒主机，为内部网络和外部网络的互相访问提供代理服务，但是来自两网络的访问都必须通过两个包过滤路由器的检查。对于向因特网公开的服务器，像 WWW、FTP、Mail 等因特网服务器也可安装在屏蔽子网内，这样无论是外部用户，还是内部用户都可访问。屏蔽子网的防火墙安全性能高，具有很强的抗攻击能力，但需要的设备多，造价高。屏蔽子网如图 5-17 所示。

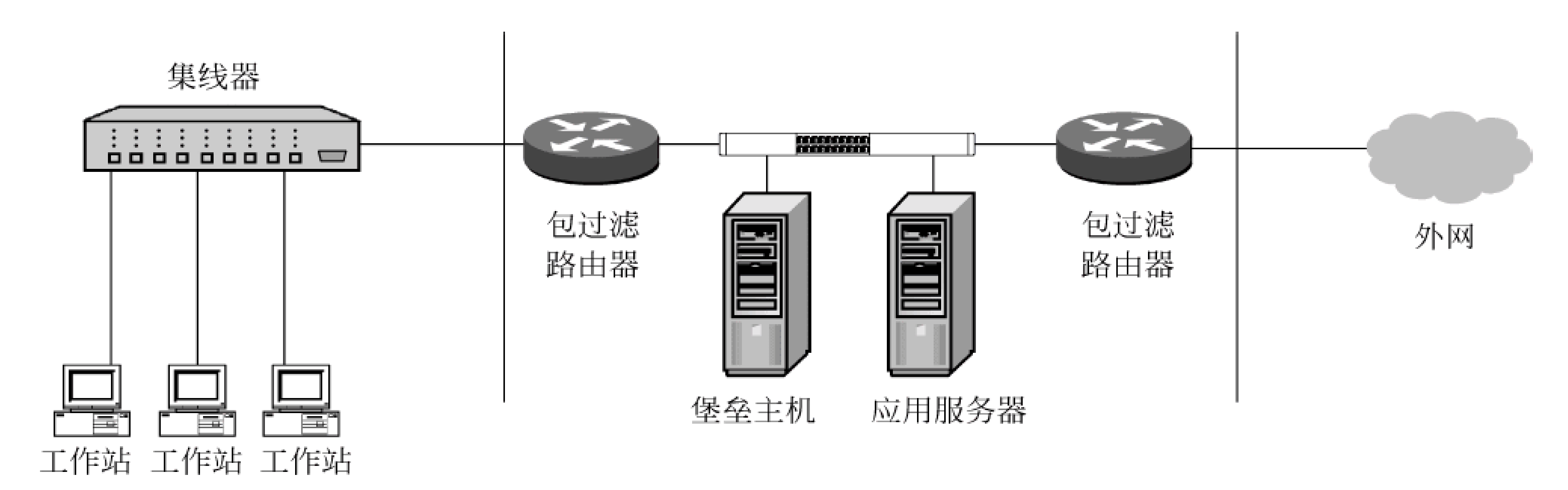


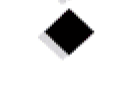
图 5-17 屏蔽子网

当然，防火墙本身也有其局限性，例如，不能防范绕过防火墙的入侵，一般的防火墙不能防止受到病毒感染的软件或文件的传输，难以避免来自内部的攻击等。总之，防火墙只是一种整体安全防范策略的一部分，仅有防火墙是不够的，安全策略还必须包括全面的安全准则，即网络访问、本地和远程用户认证、拨出拨入呼叫、磁盘和数据加密以及病毒防护等有关的安全策略。

5.3 计算机病毒

5.3.1 计算机病毒的特点及分类

计算机病毒是一种计算机程序，是一段可执行的指令代码。就像生物病毒一样，计算机病毒有独特的复制能力，可以很快地蔓延，又非常难以根除。计算机病毒不是来源于突发或偶然的原因。一次突发的停电和偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的。计算机病毒则是一段比较完美的、精巧严谨的代码，按照严格的秩序组织起来，并与所在的系统网络环境配合起来对系统进行破坏。多数计算机病毒可以找到作者信息和产地信息，通过大量的资料分析统计来看，编写计算机病毒程序的目的是多种多样的。一些天才的程序员为了表现和证明自己的能力、出于对上司的不满、为了好奇、为了祝贺和求爱等，当然也有因政治、军事、宗教、民族、专利等方面的需求而专门编写的。



计算机病毒在《中华人民共和国计算机信息系统安全保护条例》中被明确定义为："指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码"。

1. 计算机病毒的特点

计算机病毒具有很强的传染性、一定的潜伏性、特定的触发性和很大的破坏性，如图 5-18 所示。

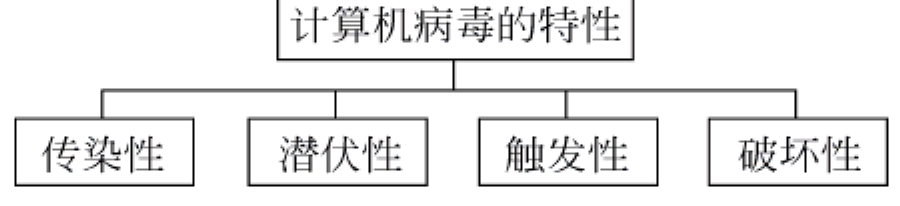


图 5-18　计算机病毒的特点

传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，病毒可得到大量繁殖，使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机感染病毒，如不及时处理，那么病毒会迅速扩散，该计算机中的大量文件(一般是可执行文件)会被感染。而被感染的文件又成了新的传染源，在与其他计算机进行数据交换或通过网络接触时，病毒会继续进行传染。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的，而计算机病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他的计算机。如果在一台计算机上发现了病毒，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台计算机联网的其他计算机可能也被该病毒传染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要的条件。

潜伏性的第一种表现是指病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘或磁带里呆上几天，甚至几年，一旦时机成熟，病毒程序得到运行机会，就要四处繁殖、扩散，继续为害。

潜伏性的第二种表现是指计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件进行加密、封锁键盘以及使系统死机等。

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

计算机病毒的破坏性主要取决于计算机病毒设计者的目的，如果病毒设计者的目的在于彻底破坏系统的正常运行，那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复，但并非所

有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染,也会导致系统崩溃等重大恶果。

2. 计算机病毒的分类

计算机病毒从不同的角度有不同的分类。按危害性分为良性病毒和恶性病毒;按寄生方式分为代替式病毒、链接式病毒、转储式病毒、填充式病毒和覆盖式病毒等。按病毒感染的途径,病毒分为4类。

(1) 操作系统型病毒(Operating System Viruses)。这类病毒程序作为操作系统的一个模块在系统中运行,一旦激发,它就工作。例如,它作为操作系统的引导程序时,计算机一旦启动就首先运行病毒程序,然后才启动操作系统程序。这类病毒也称为引导型病毒,如小球病毒、大麻病毒等。

(2) 文件型病毒(File Viruses)。文件型病毒攻击的对象是文件,并寄生在文件上。当文件运行时,首先运行病毒程序,然后才运行指定的文件(这类文件一般是可执行文件)。文件型病毒又称为外壳型(Shell Viruses)型病毒,其病毒程序包围在宿主程序的外围,对其宿主程序不修改。

感染文件的病毒有Jerusalem、Yankee Doole、Liberty、1575、Traveller、4096等,主要感染.com和.exe文件。文件型病毒增加了被感染的文件字节数,并且病毒代码主体没有加密,因此容易被查出和解除。在文件型病毒中,略有对抗反病毒手段的只有Yankee Doole病毒,当它发现用DEBUG工具跟踪时,会自动从文件中逃走。

(3) 复合型病毒。复合型病毒既感染文件,又感染引导扇区,常见的有XqR(New century)、Invader(侵入者)、Plastique(塑料炸弹)、3584(郑州狼)、ALFA/3072-2、Ghost/One Halff3544(幽灵)等。如果只解除了文件或硬盘主引导扇区的病毒,则仍会感染系统。解决的方法是从软盘启动系统,然后调用软盘版杀毒软件,同时杀掉硬盘上引导扇区病毒和文件病毒。

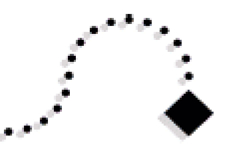
(4) 宏病毒。宏病毒主要是利用软件本身所提供的宏能力来设病毒,所以凡是具有宏能力的软件都有宏病毒存在的可能,如Word、Excel。Microsoft Word中把宏定义为:"宏就是能组织到一起作为独立的命令的一系列Word命令,它能使日常工作变得更容易。"而Word宏病毒利用Word的开放性,即Word中提供的Word Basic编程接口,并能通过DOC文档及DOC模板进行自我复制及传播。

随着Office新版本的推出,微软不断加强宏的功能,宏病毒的危害也就越来越大。Melissa病毒是利用宏来使E-mail管理程序Outlook自动根据其通讯录中记录的前50个地址发信,而July Killer宏病毒的破坏方式则是产生一个只有一句话的"deltree/y c:\"一条指令的Autoexec.bat文件来替代现有的该文件,当下次启动计算机时,这条指令就会删除C盘中的所有文件,所以宏病毒是一种危害极大的病毒。

5.3.2 计算机病毒的工作过程

1. 计算机病毒程序的结构

计算机病毒包括3大功能块,即引导模块、传播模块和破坏/表现模块。其中,后两个模块各包含一段触发条件检查代码,它们分别检查是否满足传染触发的条件和是否满足



表现触发的条件，只有在相应的条件满足时，病毒才会进行传染或表现/破坏。必须指出，不是任何计算机病毒都必须包括这 3 个模块，有些病毒没有引导模块，而有些病毒没有破坏模块。

3 个模块各自的作用是：引导模块将病毒由外存引入内存，使后两个模块处于活动状态；传播模块用来将病毒传染到其他对象上去；破坏/表现模块实施病毒的破坏作用，如删除文件、格式化磁盘等，由于该模块中有些病毒并没有明显的恶意破坏作用，只是进行一些视屏或发声方面的自我表现作用，故该模块有时又称为表现模块。计算机病毒程序结构如图 5-19 所示。

引导模块
传播模块
破坏/表现模块

图 5-19　计算机病毒程序结构

2. 计算机病毒的引导及传染

目前的计算机病毒寄生对象有两种，一是寄生在磁盘的引导区上，二是寄生在可执行文件上。

对于寄生在磁盘引导区的病毒来说，病毒引导程序占用了原引导程序的位置，并将原引导程序转移到一个特定的地方。这样系统一启动，病毒就被引导进内存并获得执行权，然后将病毒的其他两个模块装入内存，采取常驻内存技术以保证这两个模块不会被覆盖，并设定激活方式，使之能在适当的方式下被激活。然后病毒引导程序将系统引导模块装入内存，使系统在带毒状态下工作。

对于寄生在可执行文件中的病毒来说，病毒程序通过修改原有的可执行文件，一般是链接在可执行文件的首部、中间、尾部等，将病毒引导程序引导进内存，该引导程序将病毒的其他两个模块装入内存，并完成驻留内存及初始化工作，然后将执行权交给执行文件，使系统在带病毒的状态下工作。

传染是指计算机病毒由一个载体传播到另一个载体或者由一个系统进入另一个系统的过程。用户在复制磁盘或文件时，把一个病毒由一个载体复制到另一个载体上。或者是通过网络上的信息传递，把一个病毒程序从一方传递到另一方，这种传染方式叫做计算机病毒的被动传染。在病毒处于激活的状态下，只要传染条件满足，病毒程序能主动地把病毒自身传染给另一个载体或另一个系统，这种传染方式叫做计算机病毒的主动传染。

对于病毒的被动传染而言，其传染过程是随着复制磁盘或文件工作的进行而进行的。而对于计算机病毒的主动传染而言，其传染过程是这样的：在系统运行时，病毒通过病毒载体即系统的外存储器进入系统的内存储器，常驻内存，并在系统内存中监视系统的运行。

在病毒引导模块将病毒传播模块驻留内存的过程中，通常还要修改系统中断向量入口地址(例如 INT 13H 或 INT 21H)，使该中断向量指向病毒程序传播模块。这样，一旦系统执行磁盘读写操作或系统功能调用，病毒传播模块就被激活，传播模块在判断传染条件满足的条件下，利用系统 INT 13H 读写磁盘中断把病毒自身传播给被读写的磁盘或被加载的程序，也就是实施病毒的传染，然后再转移到原中断服务程序执行原有的操作。

3. 计算机病毒的触发

进入内存并处于运行状态的病毒，并不是马上就起破坏作用，还要等待一定的触发条

 件。在触发条件的设置上要兼顾潜伏性与杀伤力，过于苛刻和宽泛都会影响计算机病毒的破坏性。

计算机病毒采用的常见的触发条件有 7 种。

(1) 日期触发。许多病毒采用日期做触发条件。日期触发包括特定日期触发、月份触发、前半年后半年触发等。

(2) 时间触发。时间触发包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。

(3) 键盘触发。有些病毒监视用户的击键动作，出现病毒预定的键入时，病毒被激活，进行某些特定操作。键盘触发包括击键次数触发、组合键触发、热启动触发等。

(4) 感染触发。许多病毒的感染需要某些条件触发，而且相当数量的病毒又以与感染有关的信息反过来作为破坏行为的触发条件，称为感染触发。感染触发包括运行感染文件个数触发、感染次数触发、感染磁盘数触发、感染失败触发等。

(5) 启动触发。病毒对机器的启动次数计数，并将此值作为触发条件，称为启动触发。

(6) 访问磁盘次数触发。病毒对磁盘 I/O 访问的次数进行计数，以预定次数作为触发条件，称为访问磁盘次数触发。

(7) 调用中断功能触发。病毒对中断调用次数计数，以预定次数作为触发条件。

4. 计算机病毒的工作过程

计算机病毒的工作过程如图 5-20 所示。

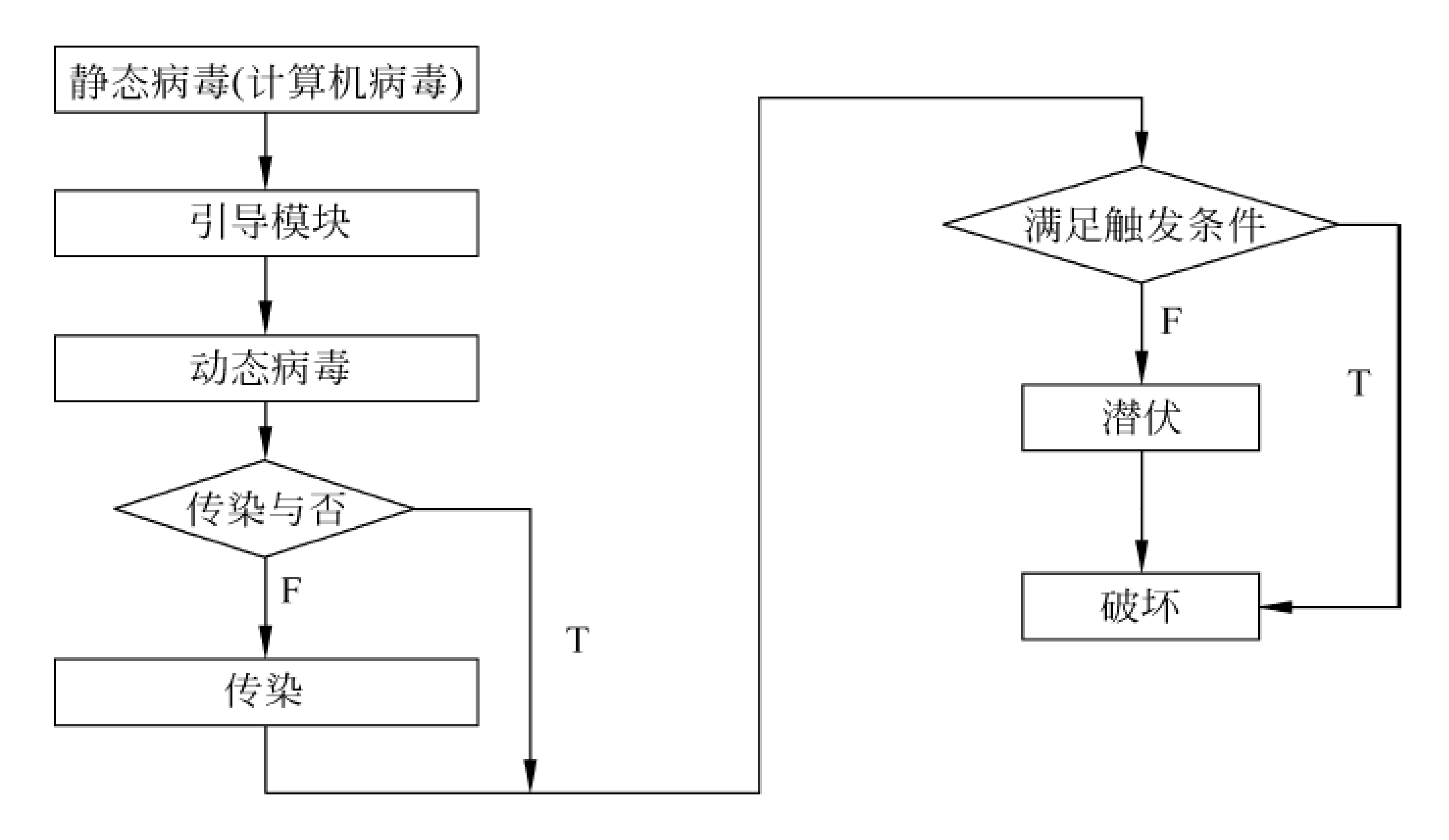


图 5-20　计算机病毒的工作过程

5.3.3　计算机防病毒技术

计算机病毒学鼻祖早在 20 世纪 80 年代初期就已经提出了计算机病毒的模型，并证明只要延用现行的计算机体系，计算机病毒就存在不可判定性。杀病毒必须先搜集到病毒样本，使其成为已知病毒，然后剖析病毒，再将病毒传染的过程准确地颠倒过来，使被感染的计算机恢复原状。因此可以看出，一方面计算机病毒是不可灭绝的，另一方面病毒也



并不可怕,世界上没有杀不掉的病毒。

1. 反病毒技术分类

从研究的角度,反病毒技术主要分 3 类。

(1) 预防病毒技术。预防病毒技术自身常驻系统内存,优先获得系统的控制权,监视和判断系统中是否有病毒存在,进而阻止计算机病毒进入计算机系统和对系统进行破坏。主要手段包括加密可执行程序、引导区保护、系统监控与读写控制等。

(2) 检测病毒技术。通过对计算机病毒的特征来进行判断的侦测技术,如自身校验、关键字等。

(3) 消除病毒技术。通过对病毒的分析,杀除病毒并恢复原文件。

2. 从具体实现技术的角度,常用的反病毒技术有 6 种

(1) 病毒代码扫描法将新发现的病毒加以分析后根据其特征编成病毒代码,加入病毒特征库中。每当执行杀毒程序时,便立刻扫描程序文件,并与病毒代码比对,便能检测到是否有病毒。病毒代码扫描法速度快、效率高。使用特征码技术需要实现一些补充功能,例如近来的压缩包、压缩可执行文件自动查杀技术。大多数防病毒软件均采用这种方法,但是该方法无法检测到未知的新病毒以及变种病毒。

(2) 人工智能陷阱法是一种监测计算机行为的常驻式扫描技术。它将所有病毒所产生的行为归纳起来,一旦发现内存的程序有任何不当的行为,系统就会有所警觉,并告知用户。其优点是执行速度快,手续简便,且可以检测到各种病毒;其缺点是程序设计难,且不容易考虑周全。

(3) 软件模拟扫描法专门用来对付千面人病毒(Polymorphic/Mutation Virus)。千面人病毒在每次传染时,都以不同的随机数加密于每个中毒的文件中,传统病毒代码比对的方式根本就无法找到这种病毒。软件模拟技术则成功地模拟 CPU 执行,在其设计的 DOS 虚拟机器(Virtual Machine)下模拟执行病毒的变体引擎解码程序,将多形体病毒解开,使其显露原来的面目,再加以扫描。目前虚拟机的处理对象主要是文件型病毒。对于引导型病毒、Word/Excel 宏病毒、木马程序在理论上都是可以通过虚拟机来处理的,但目前的实现水平仍相距甚远。就像病毒编码变形使得传统特征值方法失效一样,针对虚拟机的新病毒可以轻易使得虚拟机失效。虽然虚拟机也会在实践中不断发展。但是,PC 的计算能力有限,防病毒软件的制造成本也有限,而病毒的发展可以说是无限的。让虚拟技术获得更加实际的功效,甚至要以此为基础来清除未知病毒,其难度相当大。

(4) 先知扫描法 VICE(Virus Instruction Code Emulation)是继软件模拟技术后的一大突破。既然软件模拟可以建立一个保护模式下的 DOS 虚拟机器,模拟 CPU 动作并模拟执行程序以解开变体引擎病毒,那么类似的技术也可以用来分析一般程序检查可疑的病毒代码。因此,VICE 将工程师用来判断程序是否有病毒代码存在的方法,分析归纳成专家系统知识库,再利用软件工程的模拟技术(Software Emulation)假执行新的病毒,就可分析出新病毒代码对付以后的病毒。该技术是专门针对于未知的计算机病毒所设计的,利用这种技术可以直接模拟 CPU 的动作来侦测出某些变种病毒的活动情况,并且研制出该病毒的病毒码。由于该技术较其他解毒技术严谨,对于比较复杂的程序在病毒代码比对上会耗费比较多的时间,所以该技术的应用不那么广泛。

(5) 文件宏病毒陷阱法(MacroTrapTM)结合了病毒代码扫描与人工智能陷阱技术，根据病毒行为模式(Rule Base)来检测已知及未知的宏病毒。其中，配合对象链接与嵌套(Object Linking and Embedding)技术，可将宏与文件分开，加快扫描，并可有效地将宏病毒彻底清除。

(6) 主动内核技术(ActiveK)是将已经开发的各种网络防病毒技术从源程序级嵌入到操作系统或网络系统的内核中，实现网络防病毒产品与操作系统的无缝连接。这种技术可以保证网络防病毒模块从系统的底层内核与各种操作系统和应用环境密切协调，确保防毒操作不会伤及操作系统内核，同时确保杀灭病毒的功效。

5.3.4 计算机病毒举例

1. CIH 病毒

CIH 病毒属于文件型病毒，只感染 Windows 9x 操作系统下的可执行文件。当受感染的.exe 文件执行后，该病毒便驻留内存中，并感染所接触到的其他 PE(Portable Executable)格式执行程序。

随着技术更新的频率越来越快，主板生产厂商使用 EPROM 来做 BIOS 的存储器，这是一种可擦写的 ROM。通常所说的 BIOS 升级就是借助特殊程序修改 ROM 中 BIOS 里的固化程序。采用这种可擦写的 EPROM，虽然方便了用户及时对 BIOS 进行升级处理，但同时也给病毒带来了可乘之机。CIH 的破坏性在于它会攻击 BIOS、覆盖硬盘、进入 Windows 内核。

(1) 攻击 BIOS。当 CIH 发作时，它会试图向 BIOS 中写入垃圾信息，BIOS 中的内容会被彻底洗去。

(2) 覆盖硬盘。CIH 发作时，调节器用 IOS-Send Command 直接对硬盘进行存取，将垃圾代码以 208 个扇区为单位，循环写入硬盘，直到所有硬盘上的数据均被破坏为止。

(3) 进入 Windows 内核。无论是要攻击 BIOS，还是要设法驻留内存为病毒传播创造条件，对 CIH 这类病毒而言，关键是要进入 Windows 内核，取得核心级控制权。

为防范 CIH 病毒对计算机主板的破坏，需采取一些针对性的措施。

(1) 修改系统时间，跳过病毒的发作日。

(2) 有些计算机系统主板具备 BIOS 写保护跳线，但一般设置均为开，可将其拨至关的位置，这样可以防止病毒向 BIOS 写入信息。

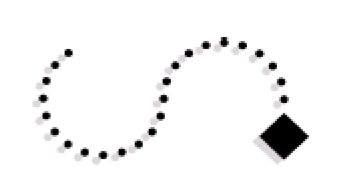
(3) 可采用压缩并解压缩文件的方式检查 CIH 病毒，如果解压缩出现问题，多半可以肯定有 CIH V1.2 病毒的存在，但用该方法不能判断文件中是否存在 CIH V1.4 病毒。

(4) 用户不要轻易运行从电子邮件或网站上下载的未知软件。

(5) 由于病毒是将垃圾码写入硬盘，导致硬盘的数据不能恢复，务必将重要数据备份，以免造成损失。

2. 蠕虫病毒

蠕虫病毒的编写相对其他形式的病毒程序来说简单一些，它可以用 VB 语言、C 语言或者传统语言来编写，还可以利用 wsh 脚本宿主，用常见的 VBscript 和 Javascript 等语言来编写。但这并不意味着这种程序的破坏性小，相反，它具有极强的破坏能力，并且由



于有因特网这个传播的大好场所，蠕虫病毒有着将传统病毒挤出市场的趋势。

蠕虫病毒与一般的计算机病毒不同，它不是将自身复制并附加到其他程序中，所以在病毒中也算是一个另类。包括蠕虫病毒在内的脚本病毒是很容易制造的。其利用了 Windows 系统的开放性，特别是 com 到 com^{+} 的组件编程思路，一个脚本程序调用功能更大的组件来完成自己的功能。它们相对来说较其他的病毒容易编写。

蠕虫病毒与普通病毒的区别如表 5-4 所示。

表 5-4　蠕虫病毒与普通病毒的区别

特性＼类别	普通病毒	蠕虫病毒
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

5.4　黑客的攻击技术简介

黑客是英文 hacker 的音译，hacker 这个单词源于动词 hack，原是指热心于计算机技术且水平高超的计算机专家，尤其是程序设计人员。他们非常精通计算机硬件和软件知识，对操作系统和程序设计语言有着全面深刻地认识，善于探索计算机系统的奥秘，发现系统中的漏洞及原因所在。他们信守永不破坏任何系统的原则，检查系统的完整性和安全性，并乐于与他人共享研究成果。

到今天，黑客一词已被用于泛指那些未经许可就闯入计算机系统进行破坏的人。他们中的一些人利用漏洞进入计算机系统后，破坏重要的数据。另一些人利用黑客技术控制别人的计算机，从中盗取重要资源，干起了非法的勾当。他们已经成了入侵者和破坏者。

造成网络不安全的主要因素是系统、协议及数据库等存在设计上的缺陷。当今的计算机网络操作系统在结构设计和代码设计时，偏重考虑系统使用时的方便性，导致系统在远程访问、权限控制和口令管理等许多方面存在安全漏洞。网络互联一般采用 TCP/IP 协议，它是一个工业标准的协议簇，但该协议簇在制订之初对安全问题考虑不多，协议中有很多的安全漏洞。同样，数据库管理系统（DBMS）也存在数据的安全性、权限管理及远程访问等方面问题。例如，在 DBMS 或应用程序中可以预先安装从事情报收集、受控激发、定时发作等破坏程序。

5.4.1　黑客的进攻过程

黑客的进攻过程如图 5-21 所示。

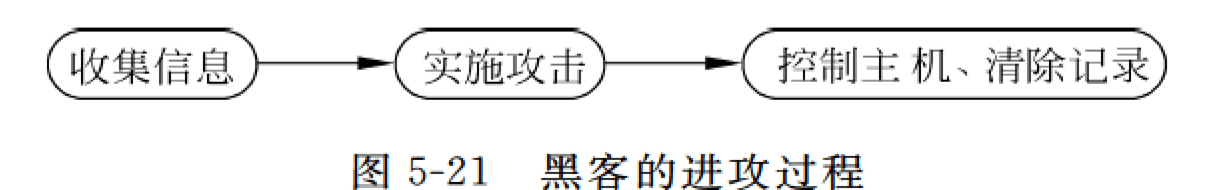


图 5-21　黑客的进攻过程

1. 收集信息

黑客在发动攻击前需要锁定目标，了解目标的网络结构，收集目标系统的各种信息等。

（1）锁定目标。网络上有许多主机，黑客首先要寻找目标站点。能真正标识主机的是 IP 地址，黑客利用域名和 IP 地址就可以顺利地找到目标主机。

（2）了解目标的网络结构。确定要攻击的目标后，黑客就会设法了解其所在的网络结构，哪里是网关、路由，哪里有防火墙，哪些主机与要攻击的目标主机关系密切等，最简单的方法就是用 tracert 命令追踪路由，也可以发一些数据包看其是否能通过，猜测其防火墙过滤原则的设定等。当然老练的黑客在干这些的时候都会利用别的计算机来间接地探测，从而隐藏他们真实的 IP 地址。

（3）收集系统信息。在收集到目标的网络信息之后，黑客会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。收集系统信息的方法有：开放端口分析、利用信息服务和利用扫描器。

首先黑客要知道目标主机采用的是什么操作系统的什么版本，如果目标主机开放 Telnet 服务，黑客只要 Telnet 目标主机，就会显示目标主机系统的登录提示信息；接着黑客还会对其开放端口进行服务分析，看是否有能被利用的服务。WWW、Mail、FTP、Telnet 等日常网络服务都有开放的端口，通常情况下 Telnet 服务的端口是 23，WWW 服务的端口是 80，FTP 服务的端口是 23。

利用信息服务，像 SNMP 服务、Traceroute 程序、Whois 服务可以查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。Traceroute 程序能够获得到达目标主机所要经过的网络数和路由器数。Whois 协议服务能提供所有有关的 DNS 域和相关的管理参数。Finger 协议可以用 Finger 服务来获取一个指定主机上的所有用户的详细信息（如用户注册名、电话号码、最后注册时间以及用户有没有读邮件等），所以如果没有特殊的需要，管理员应该关闭这些服务。

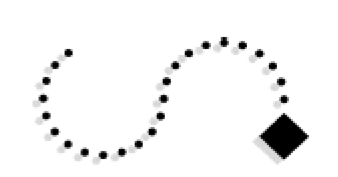
黑客收集系统信息当然少不了利用扫描器来帮他们发现系统的各种漏洞，包括各种系统服务漏洞、应用软件漏洞、CGI、弱口令用户等。

2. 实施攻击

当黑客探测到了足够的系统信息，对系统的安全弱点有了了解后就会发动攻击，当然他们会根据不同的网络结构、不同的系统情况而采用不同的攻击手段。一般黑客攻击的终极目的是能够控制目标系统，窃取其中的机密文件，但并不是每次黑客攻击都能够达到控制目标主机的目的，所以有时黑客也会发动拒绝服务攻击之类的干扰攻击，使系统不能正常工作。

3. 控制主机并清除记录

黑客利用种种手段进入目标主机系统并获得控制权之后，不会马上进行破坏活动，例如，删除数据、涂改网页等。黑客为了能长时间地保留和巩固他对系统的控制权，不被管理员发现，他会做两件事：清除记录和留下后门。日志往往会记录一些黑客攻击的蛛丝马迹，黑客当然不会留下这些“犯罪证据”，他会删除日志或用假日志覆盖它。为了日后可以不被觉察地再次进入目标主机的系统，黑客会更改某些系统设置，在系统中置入特洛伊



木马或其他一些远程操纵程序，也可能是什么都不动，只是把目标主机的系统作为他存放黑客程序或资料的仓库，还可能利用这台已经攻陷的主机去继续他下一步的攻击，继续入侵内部网络，或者利用这台主机发动 DOS 攻击使网络瘫痪。

5.4.2 黑客常用的攻击方法

计算机系统中存在的安全隐患是黑客进行攻击的地方，黑客创造了多种攻击方法，常用的攻击方法如图 5-22 所示。

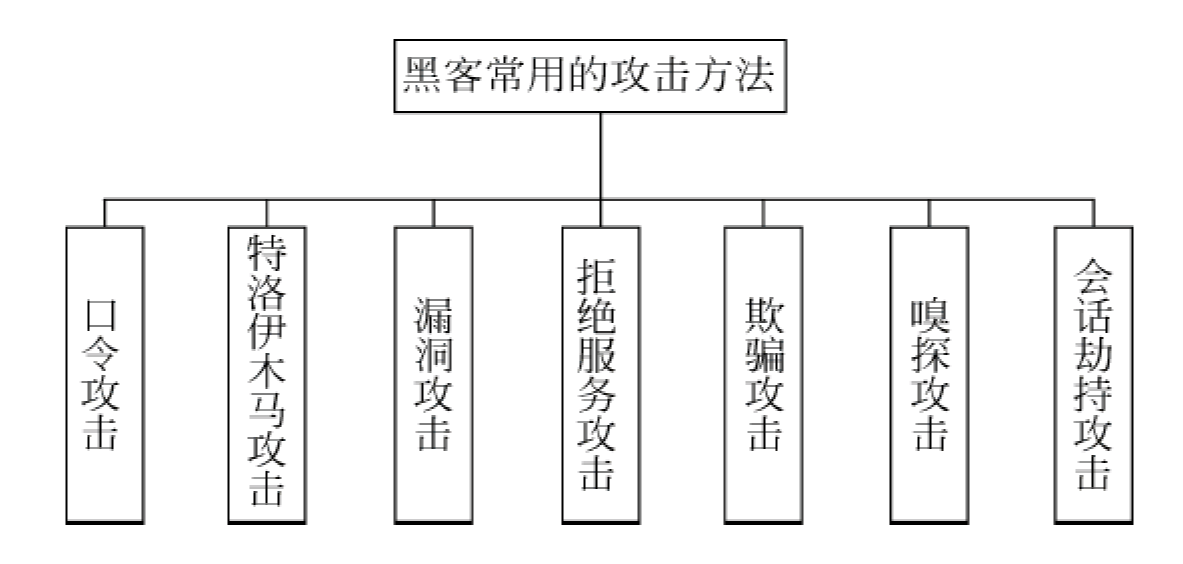


图 5-22 黑客常用的攻击方法

1. 口令攻击

口令攻击是黑客的最常用的攻击方法，从黑客诞生的那天起口令攻击就开始被使用，这种攻击方式有 3 种方法。

(1) 暴力破解法。黑客在知道用户的账号后用一些专门的软件强行破解用户口令(包括远程登录破解和对密码存储文件 Passwd、Sam 的破解)。采用这种方法进行攻击的黑客要有足够的耐心和时间，但总有一些使用简单口令的用户账号，使得黑客可以迅速将其破解。

(2) 伪造登录界面法。在被攻击主机上启动一个可执行程序，该程序显示一个伪造的登录界面，当用户在这个伪造的界面上键入用户名和密码后，程序将用户输入的信息传送到攻击者主机。

(3) 通过网络监听得到用户口令。这种方法危害性很大，监听者往往能够获得某一个网段的所有用户账号和口令。

2. 特洛伊木马攻击

特洛伊木马程序攻击也是黑客常用的攻击手段。黑客会编写一些看似"合法"的程序，但实际上此程序隐藏有其他非法功能，例如，用户运行一个外表看似是一个有趣的小游戏的程序时，该程序却在后台为黑客创建了一条访问该用户系统的通道，这就是特洛伊木马程序。当然只有当用户运行了木马程序后，黑客才能对用户系统进行攻击，所以黑客会把木马程序上传到一些站点引诱用户下载，或者用 E-mail 寄给用户并编造各种理由骗用户运行它，当用户运行此软件后，该软件会悄悄执行它的非法功能：跟踪用户的计算机操作，记录用户输入的口令、上网账号等敏感信息，并把信息发送到黑客指定的电子信箱中。如果是像冰河、灰鸽子这样的功能强大的远程控制木马，黑客还可以像在本地操作一样远程操控用户的计算机。

3. 漏洞攻击

利用漏洞攻击是黑客攻击中最容易得逞的方法。许多系统及网络应用软件都存在着各种各样的安全漏洞，如 Windows 98 的共享目录密码验证漏洞，Windows 2000 的 Unicode、printer、ida、idq、webdav 漏洞，UNIX 的 Telnet、RPC 漏洞、Sendmail 的邮件服务软件漏洞，还有基于 Web 服务的各种 CGI 漏洞等，这些都是最容易被黑客利用的系统漏洞，特别是其中的一些缓冲区溢出漏洞。利用缓冲区溢出漏洞，黑客不但可以通过发送特殊的数据包来使服务或系统瘫痪，甚至可以精确地控制溢出后在堆栈中写入的代码，使其能执行黑客的任意命令，从而进入并控制系统。

4. 拒绝服务攻击

拒绝服务攻击(DoS)是一种最悠久也是最常见的攻击形式，它利用 TCP/IP 协议的缺陷，将提供服务的网络的资源耗尽，导致网络不能提供正常服务，是一种对网络危害巨大的恶意攻击。其实严格来说拒绝服务攻击并不是某一种具体的攻击方式，而是攻击所表现出来的结果，最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。DoS 的攻击方法可以是单一的手段，也可以是多种方式的组合利用，不过其结果都是一样的，即合法的用户无法访问所需信息。

通常单一的拒绝服务攻击可分为两种类型：一种攻击是黑客利用网络协议缺陷或系统漏洞发送一些非法的数据或数据包，使得系统死机或重新启动，从而使一个系统或网络瘫痪，如 Land 攻击、WinNuke、Ping of Death、TearDrop 等；另一种攻击是黑客在短时间内发送大量伪造的连接请求报文到网络服务所在的端口，例如 80 端口，从而消耗系统的带宽或设备的 CPU 和内存，造成服务器的资源耗尽，系统停止响应甚至崩溃，其中，具有代表性的攻击手段包括 SYN flood、ICMP flood、UDP flood 等。

分布式拒绝服务(DDoS)攻击是目前网络的头号威胁，是在传统的 DoS 攻击基础之上产生的一种攻击方式。单一的 DoS 攻击一般采用一对一攻击，而分布式的拒绝服务攻击是黑客控制多台计算机(可以是几台也可以是成千上万台)同时攻击，这样的攻击即使是一些大网站也很难抵御。

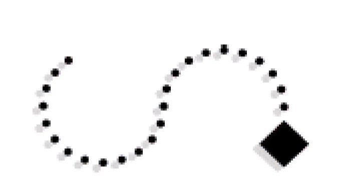
5. 欺骗攻击

常见的黑客欺骗攻击方法有：IP 欺骗攻击、DNS 欺骗邮件欺骗攻击和网页欺骗攻击等。

(1) IP 欺骗攻击。黑客改变自己的 IP 地址，伪装成别人计算机的 IP 地址来获得信息或者得到特权。如 UNIX 计算机之间能建立信任关系，使得这些主机的访问变得容易，而这种信任关系基本上是通过 IP 地址进行验证，这样就知道 IP 欺骗做什么了。

(2) 电子邮件欺骗攻击。黑客向某位用户发了一封电子邮件，并且修改了邮件头信息(使得邮件地址看上去和这个系统管理员的邮件地址完全相同)，信中他冒称自己是系统管理员，说由于系统服务器故障导致部分用户数据丢失，要求该用户把他的个人信息马上用 E-mail 回复给他，这就是一个典型的电子邮件欺骗攻击。

(3) 网页欺骗攻击。黑客将某个站点的网页都复制下来，修改其链接，使得用户访问这些链接时先经过黑客控制的主机，然后黑客会想方设法让用户访问这个修改后的网页，他则监控用户整个 HTTP 请求过程，窃取用户的账号和口令等信息，甚至假冒用户给服



务器发送和接收数据。如果这个网页是电子商务站点，那用户的损失可想而知。

6. 嗅探攻击

要了解嗅探攻击方法，首先要知道它的原理。网络的一个特点就是数据总是在流动中，当数据从网络的一台计算机到另一台计算机的时候，通常会经过大量不同的网络设备，在数据传输过程中，有人可能会通过特殊的设备（嗅探器，有硬件和软件两种）捕获这些传输网络数据的报文，这就是嗅探攻击。

嗅探攻击主要有两种途径。一种是针对简单的采用集线器（Hub）连接的局域网，黑客只要把嗅探器安装到这个网络中的任何一台计算机上就可以实现对整个局域网的侦听，这是因为共享 Hub 获得一个子网内需要接收的数据时，并不是直接发送到指定主机，而是通过广播方式发送到每台计算机。正常情况下，数据接受的目标计算机会处理该数据，而其他非接受者的计算机就会过滤这些数据，但安装了嗅探器的计算机则会接受所有数据。另一种是针对交换网络的，由于交换网络的数据是从一台计算机发送到预定的计算机，而不是广播的，所以黑客必须将嗅探器放到像网关服务器、路由器这样的设备上才能监听到网络上的数据。当然这比较困难，但一旦成功就能够获得整个网段的所有用户账号和口令，所以黑客还是会通过其他种种攻击手段来实现它，如通过木马方式将嗅探器发给某个网络管理员，使其不自觉地为攻击者安装嗅探器。

7. 会话劫持攻击

假设某黑客在暗地里等待某位合法用户通过 Telnet 远程登录到一台服务器上，当这位用户成功地提交密码后，黑客就开始接管该用户当前的会话并摇身变成了这个用户，这就是会话劫持攻击。在一次正常的通信过程中，黑客作为第三方参与到其中，或者是在数据流（例如基于 TCP 的会话）里注射额外的信息，或者是将双方的通信模式暗中改变，即从直接联系变成有黑客联系。会话劫持是一种结合了嗅探以及欺骗技术在内的攻击手段，最常见的是 TCP 会话劫持，像 HTTP、FTP、Telnet 都可能被进行会话劫持。

要实现会话劫持，黑客首先必须窥探到正在进行 TCP 通信的两台主机之间传送的报文源 IP、源 TCP 端口号、目的 IP、目的 TCP 端号，从而推算出其中一台主机将要收到的下一个 TCP 报文段中的 seq 和 ackseq 值，这样在该合法主机收到另一台合法主机发送的 TCP 报文前，攻击者根据所截获的信息向该主机发出一个带有净荷的 TCP 报文，如果该主机先收到攻击报文，就可以把合法的 TCP 会话建立在攻击主机与被攻击主机之间。带有净荷的攻击报文能够使被攻击主机对下一个要收到的 TCP 报文中的确认序号（ackseq）的值发生变化，从而使另一台合法的主机向被攻击主机发出的报文被拒绝。

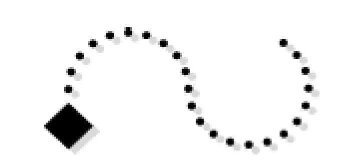
会话劫持攻击避开了被攻击主机对访问者的身份验证和安全认证，从而使黑客能直接进入被攻击主机，对系统安全构成的威胁比较严重。实现会话劫持攻击不但需要复杂的技术，而且还需要精确把握攻击时间，所以会话劫持攻击并不是太常见。

5.4.3 黑客的常用工具

黑客工具是指编写出来的用于网络安全方面的工具软件，其功能是支持网络攻击过程。下面对黑客的常用工具进行简单的介绍。

1. 扫描类软件

通过扫描程序，黑客可以找到攻击目标的 IP 地址、开放的端口号、服务器运行的版



本、程序中可能存在的漏洞等。根据不同的扫描目的，扫描类软件又分为地址扫描器、端口扫描器、漏洞扫描器3个类别。在很多人看来，这些扫描器获得的信息大多数都是没有用处的，然而在黑客看来，扫描器好比黑客的眼睛，它可以让黑客清楚地了解目标，有经验的黑客则可以将目标"摸得一清二楚"，这对于攻击来说是至关重要的。同时扫描器也是网络管理员的得力助手，网络管理员可以通过扫描器了解自己系统的运行状态和可能存在的漏洞，在黑客"下手"之前将系统中的隐患清除，保证服务器的安全稳定。扫描类软件有流光、SuperScan、X-way等。SuperScan软件的界面如图5-23所示。



图5-23　SuperScan软件的界面

2. 远程监控类软件

远程监控类软件也叫做木马程序，这种程序实际上是在服务器上运行一个客户端软件，而在黑客的计算机中运行一个服务端软件，如此一来，服务器将会变成黑客的服务器的"手下"，也就是说黑客将会利用木马程序在服务器上开一个端口，通过这种特殊的木马功能对服务器进行监视、控制。因此，只要黑客掌握了某个木马的使用和操作方法，就可以轻易接管网络服务器或者其他上网者的计算机。

在控制了服务器之后，黑客的攻击行动也就接近尾声了，然而在攻击之前，黑客必须想办法让服务器运行木马的客户端程序，这就需要利用漏洞或者进行欺骗。远程监控类软件有冰河、灰鸽子等。冰河软件的界面如图5-24所示。

3. 系统攻击和密码破解类软件

这类软件大多数都是由高级黑客编写出来供初级黑客使用的现成软件，软件本身不需要使用者具备太多的知识，使用者只要按照软件的说明操作就可以达到软件的预期目的。



图 5-24　冰河软件的界面

系统攻击类软件主要分为信息炸弹和破坏炸弹。网络上常见的垃圾电子邮件就是这种软件的“杰作”，还有聊天室中经常看到的“踢人”、“骂人”类软件、论坛的垃圾灌水器、系统蓝屏炸弹也都属于此类软件的变异形式。

密码破解类软件可以帮助黑客寻找系统登录密码，相对于利用漏洞暴力破解密码要简单许多，但效率非常低，黑客无论是使用密码破解软件还是利用漏洞进入系统之后，都达到了入侵的目的。

常用的系统攻击和密码破解类软件有溯雪、黑雨、网络刺客Ⅱ等。网络刺客Ⅱ软件的界面如图 5-25 所示。



图 5-25　网络刺客Ⅱ软件界面

4. 监听类软件

通过监听，黑客可以截获网络的信息包，之后对加密的信息包进行破解，进而分析包内的数据，获得有关系统的信息；也可以截获个人上网的信息包，获得用户的上网账号、系统账号、电子邮件账号等个人隐私资料。监听类软件有 Sinffit、nc 和 CaptureNet 等。CaptureNet 软件的界面如图 5-26 所示。

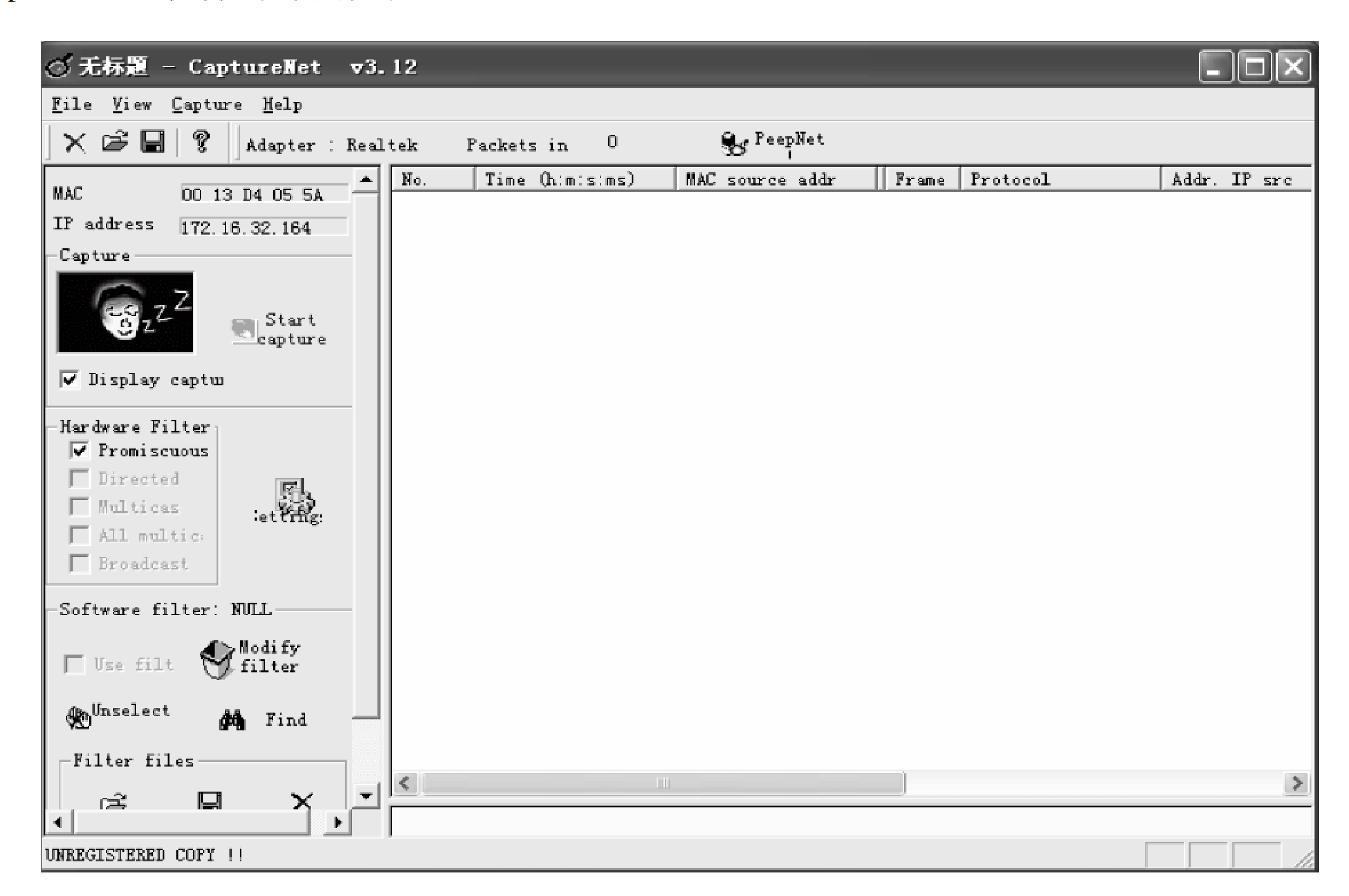


图 5-26 CaptureNet 软件界面

5.5 本章小结

本章主要介绍了加强计算机网络系统安全性的主要方法和技术手段。

在增强操作系统安全性上，主要学习了 Windows 2003 在域模式下提高系统安全性的主要技术手段：身份认证和访问控制。这些工作都是操作系统在后台自动进行的，是网络环境下进行资源共享、信息共享的基础，对于它的学习有助于我们理解与之相关的网络设置和网络编程。

在增强系统安全性上，主要介绍了计算机病毒的特点、工作原理及常用的防病毒技术。同时还介绍了防火墙技术以及常用的防火墙的体系结构，通过学习了解到防火墙是进行内、外网分隔的有效工具，同时体会到防病毒软件与防火墙在提高计算机网络安全性上的不同功用。最后简单介绍了破坏计算机网络系统的人——黑客，以及黑客常用的进攻手段和进攻过程。

5.6　本章习题

1. 简述 Windows 2003 进行身份认证的基本过程。
2. 简述计算机病毒的基本工作过程及主要的防病毒技术。
3. 简述防火墙的工作原理及体系结构。
4. 简述 CIH 病毒与蠕虫病毒的区别。

第 6 章

网络安全工具的使用

【本章内容】

作为第 5 章的实训环节，本章主要介绍常见的增强计算机网络系统安全性软件的使用方法。通过防火墙软件、防病毒软件的使用，进一步深化对第 5 章知识的理解，同时介绍了黑客基于局域网的攻防过程和配置服务器时应注意的问题。

【本章重点】

① 掌握常见防火墙的使用方法。
② 学会使用服务器版杀毒软件。
③ 了解黑客攻击的一般流程，以及一些防御手段。
④ 知道保证服务器安全的一些常规设置。
⑤ 体会软件中相关设置的修改对计算机网络安全性的影响。

本章主要介绍增强计算机网络安全性的一些常用软件的使用方法，例如，防火墙软件及防病毒软件。通过这些软件的学习与使用，增强对于网络安全的基础知识的理解，体会软件相关设置的修改可能对系统安全性造成的影响，进而能够按照用户的需求建立一个完整的、安全的网络系统。本章还介绍了一个基于局域网的简单的黑客攻击过程，希望读者能从正反两个方面认识计算机网络安全的重要性。

6.1 防火墙软件的使用案例

6.1.1 Windows Server 2003 防火墙

Windows Server 2003 自带的防火墙叫做 Internet 连接防火墙(ICF)，是一种防火墙软件，可以拦截来自网络中的非法通信。Internet 连接防火墙允许安全的网络通信进入网络系统，同时拒绝不安全的通信进入，从而使网络系统免受外来威胁。Internet 连接防火墙、Internet 连接共享和网桥功能只包含在 Windows Server 2003 Standard Edition 和 32 位版本的 Windows Server 2003 Enterprise Edition 中。在 Windows Server 2003 Web Edition、32 位版本的 Windows Server 2003 Datacenter Edition 和 64 位版本的 Windows

Server 2003 中不包含这两个功能。

1. 启用 Internet 连接防火墙

在“控制面板”窗口中单击“网络连接”图标，在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单中选择“属性”命令，系统将弹出“本地连接 属性”对话框，如图 6-1 所示。

在“本地连接 属性”对话框的“高级”选项卡中单击“设置”按钮，弹出“Windows 防火墙”对话框，如图 6-2 所示。



图 6-1　“本地连接 属性”对话框

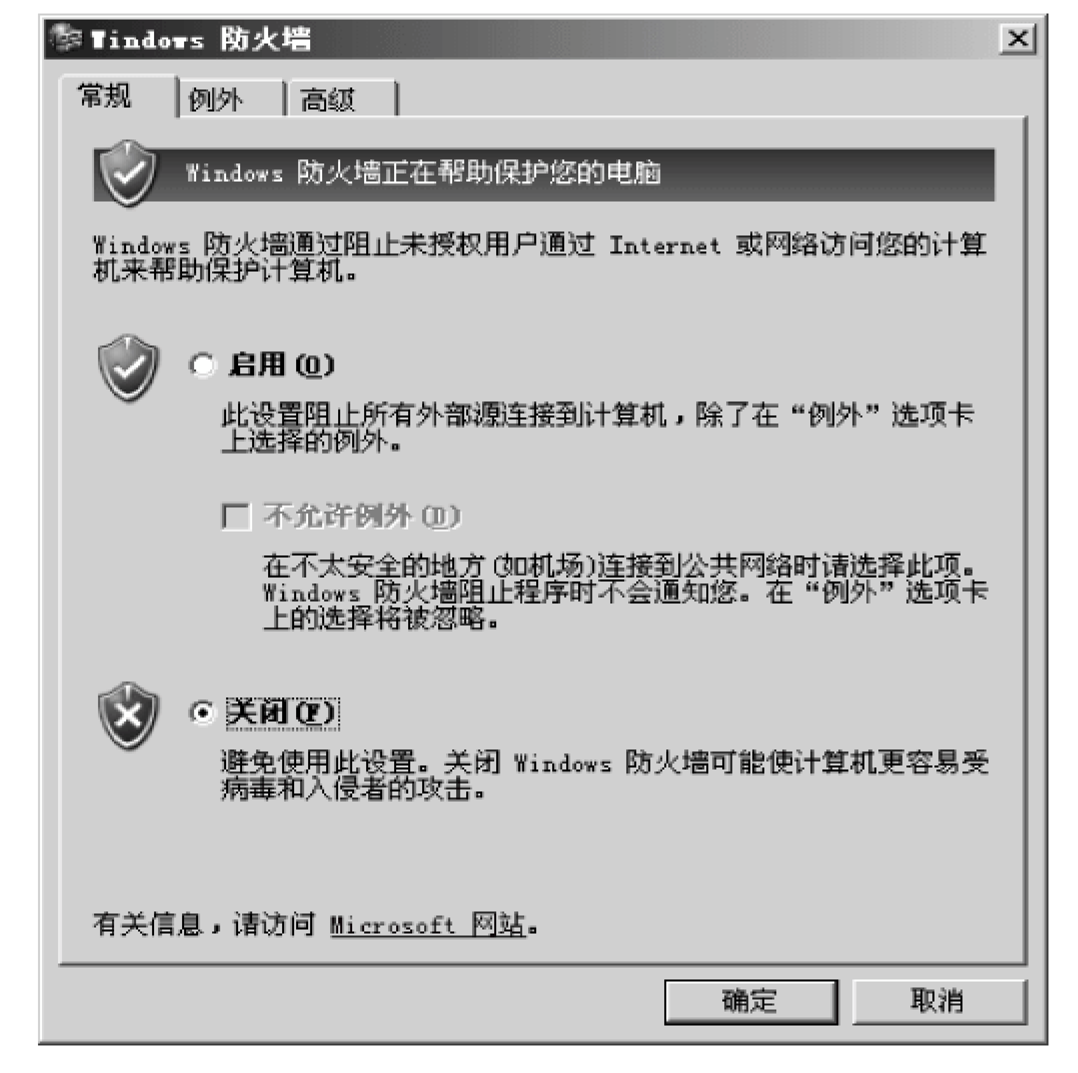


图 6-2　“Windows 防火墙”对话框

系统默认防火墙是关闭的，在“Windows 防火墙”对话框中选中“启用”单选按钮，单击“确定按钮”，便可以启动 Internet 连接防火墙。启动 Internet 连接防火墙之后，在“网络连接”窗口中的“本地连接”图标将变为，网络中的其他用户将不能够访问系统所提供的服务。

2. 添加允许通过防火墙的端口

为了使网络中的安全服务能够通过某些端口访问本系统，可以在“Windows 防火墙”对话框的“例外”选项卡中添加允许通过防火墙访问系统的程序和端口，如图 6-3 所示。

例如，诺顿杀毒软件在漫游客户端时是通过 1056 端口连接到服务器的。在“例外”选项卡中单击“添加端口”按钮，在弹出的“添加端口”对话框中添加 1056 端口，单击“确定”按钮，从而使诺顿服务可以通过防火墙，如图 6-4 所示。

3. 添加允许通过防火墙的服务

Internet 连接防火墙在没有添加服务之前，服务器所提供的任何服务都不允许网络中的计算机访问，例如 Web 服务。为了使其他计算机能够访问服务器的 Web 服务，就必须在 Internet 连接防火墙中进行添加。




图 6-3 “例外”选项卡

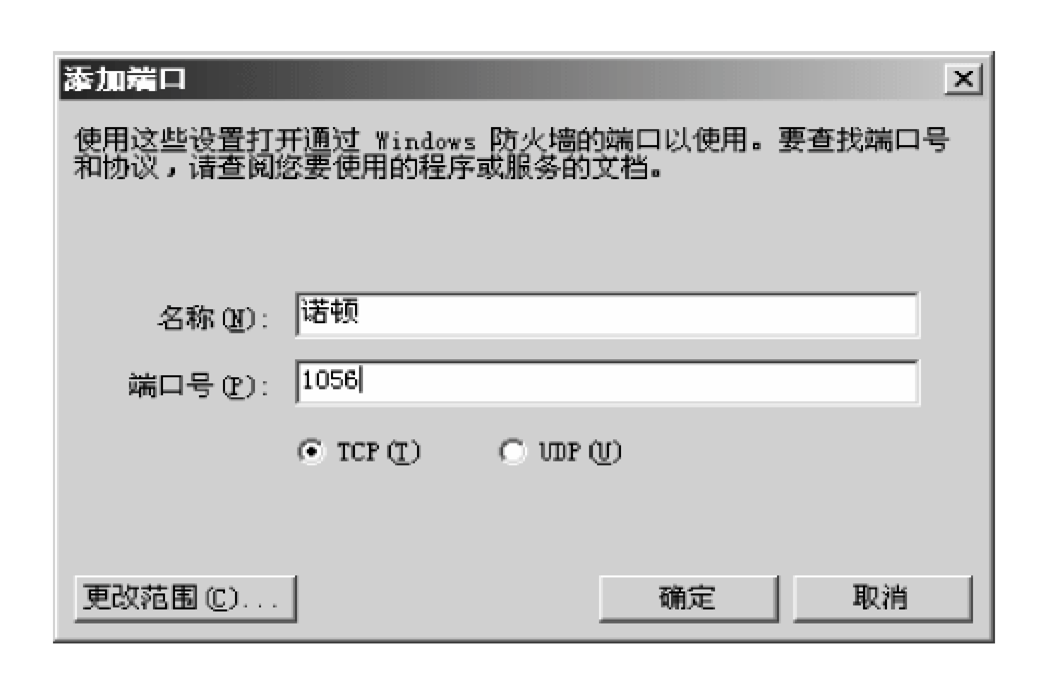


图 6-4 “添加端口”对话框

在“Windows 防火墙”对话框的“高级”选项卡中选择对外服务的网络连接，如图 6-5 所示。

在“高级”选项卡的“网络连接设置”选项组中单击“设置”按钮，弹出“高级设置”对话框，如图 6-6 所示。在该对话框中选择“Web 服务器(HTTP)”复选框，单击“确定”按钮，网络中的其他计算机就可以访问服务器所提供的 Web 服务了。



图 6-5 “高级”选项卡

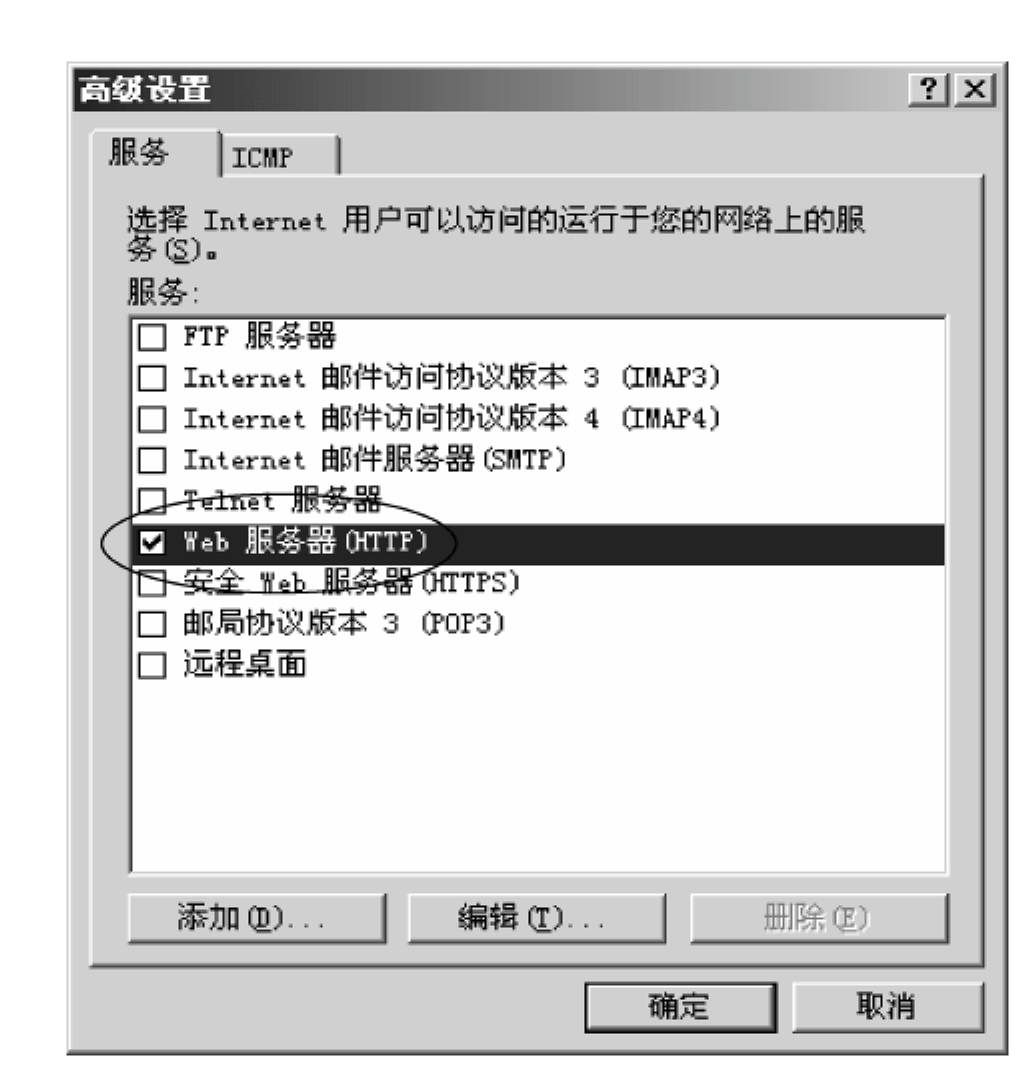
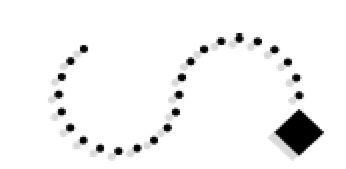


图 6-6 “高级设置”对话框



4. 添加允许通过防火墙的响应请求

在添加了 Web 服务以后，网络中的其他计算机虽然能够访问服务器的 Web 服务，但是其他计算机在 DOS 窗口中使用 Ping 命令时，会返回 Request timed out. 的信息，表示这个服务器是禁 Ping 的。

要使服务器能够响应 Ping 命令，需要在“高级设置”对话框的 ICMP 选项卡中选择“允许传入响应请求”复选框，如图 6-7 所示，单击“确定”按钮就可以了。

图 6-8 所示为允许 Ping 命令之前客户端返回服务器所响应的数据，图 6-9 所示为允许 Ping 命令之后客户端返回服务器所响应的数据。

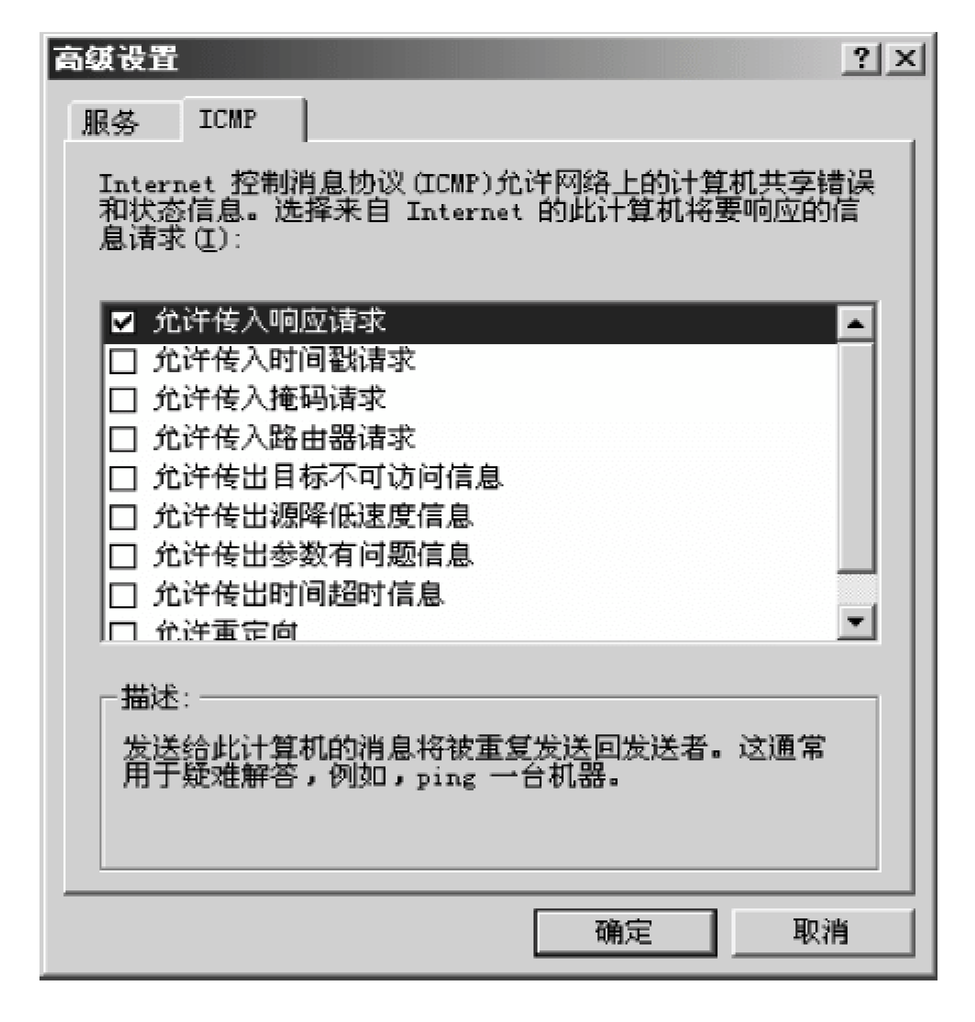


图 6-7　ICMP 选项卡

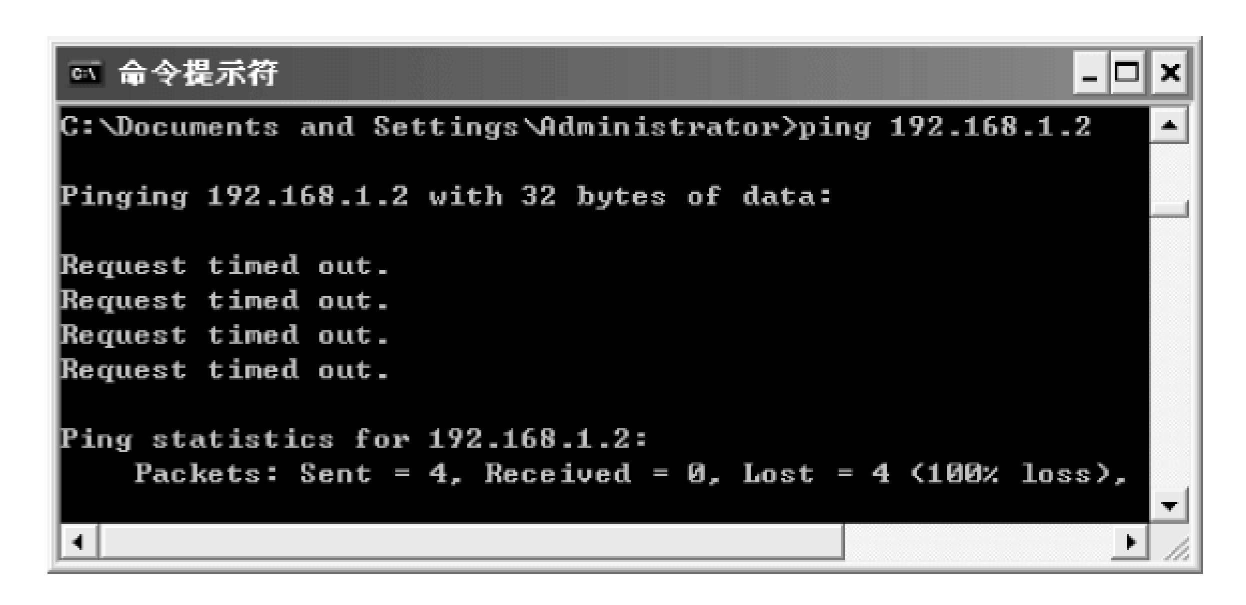


图 6-8　允许 Ping 命令之前客户端返回服务器所响应的数据

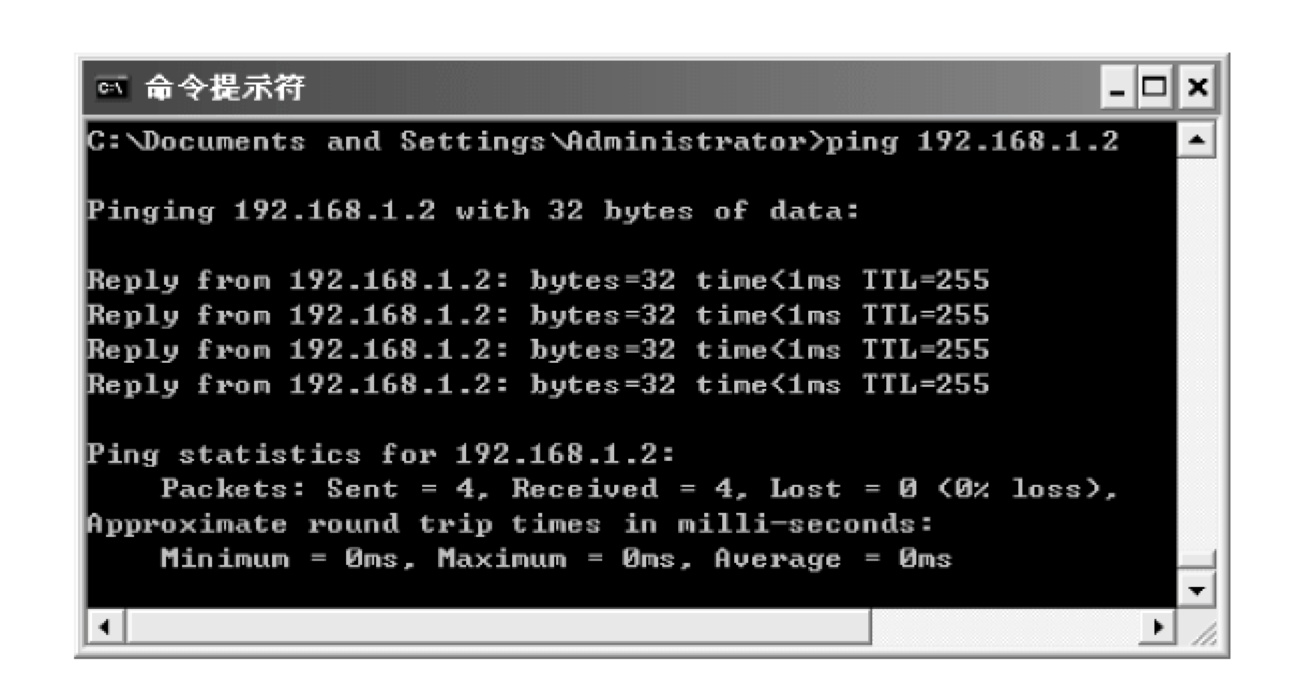


图 6-9　允许 Ping 命令之后客户端返回服务器所响应的数据

6.1.2　天网防火墙

天网防火墙是国内外针对个人用户最好的中文软件防火墙之一。在目前网络受攻击案件数量直线上升的情况下，用户随时都可能遭到各种恶意攻击，这些恶意攻击可能导致

用户的上网账号被窃取和冒用、银行账号被盗用、电子邮件密码被修改、财务数据被利用、机密档案丢失、隐私曝光等,甚至黑客(Hacker)或刽客(Cracker)能通过远程控制删除用户硬盘上所有的资料数据,使用户整个计算机系统架构全面崩溃。为了抵御黑客或刽客的攻击,建议用户在个人计算机上安装一套天网防火墙个人版,它能拦截一些来历不明、有害敌意访问或攻击行为。图 6-10 所示为"天网防火墙个人版"应用程序界面。



图 6-10 "天网防火墙个人版"应用程序界面

1. 安全级别设置

天网防火墙个人版的预设安全级别分为低、中、高、扩展和自定义 5 个等级,默认的安全等级为中级,下面介绍各个级别所代表的含义。

(1) 低。所有应用程序初次访问网络时都将询问,已经被认可的程序则按照设置的相应规则运作。用户的计算机将完全信任局域网,允许局域网内部的机器访问自己提供的各种服务(文件、打印机共享服务),但禁止互联网上的机器访问这些服务。该级别适用于在局域网中提供服务的用户。

(2) 中。所有应用程序初次访问网络时都将询问,已经被认可的程序则按照设置的相应规则运作。禁止访问系统级别的服务(如 HTTP、FTP 等)。局域网内部的机器只允许访问文件、打印机共享服务。使用动态规则管理,允许授权运行的程序开放的端口服务,例如,网络游戏或者视频语音电话软件提供的服务。该级别适用于普通个人上网用户。

(3) 高。所有应用程序初次访问网络时都将询问,已经被认可的程序则按照设置的相应规则运作。禁止局域网内部和互联网上的机器访问自己提供的网络共享服务(文件、打印机共享服务),局域网和互联网上的机器将无法看到本机器。除了已经被认可的程序打开的端口,系统会屏蔽掉向外部开放的所有端口。该级别是最严密的安全级别。

(4) 扩展。基于中安全级别,再配合一系列专门针对木马和间谍程序的扩展规则,可以防止木马和间谍程序打开 TCP 或 UDP 端口,监听甚至开放未许可的服务。可以根据最新的安全动态对规则库进行升级。该级别适用于需要频繁试用各种新的网络软件和服务且需要对木马程序进行足够限制的用户(试用版用户不享受这项服务)。

(5) 自定义。如果用户了解各种网络协议,可以自己设置规则。注意,规则设置不正确会导致无法访问网络。该级别适用于对网络有一定了解并需要自行设置规则的用户。

2. IP 规则设置

IP 规则是针对整个系统的网络层数据包监控而设置的。利用自定义 IP 规则,可以针对不同的网络状态,设置 IP 安全规则。在"天网防火墙个人版"窗口中单击"IP 规则管理"按钮或者在"安全级别"中选中"自定义"单选按钮,进行 IP 规则的设置,如图 6-11 所示。

需要注意的是,在设置 IP 规则时要尽量将允许的 IP 规则放在禁止的 IP 规则之前,



图 6-11　IP 规则设置

这样天网防火墙个人版在匹配了允许的 IP 规则之后，不会去检测禁止的 IP 规则，这样可以提高 IP 规则的运行效率。

6.2　防病毒软件的使用案例及经验

6.2.1　诺顿杀毒软件的使用方法

1. 诺顿杀毒软件(Symantec)的更新

在默认安装的情况下，诺顿杀毒软件的更新被调度为在每周五晚上 8 点自动运行。在运行调度更新时，计算机必须正在运行并且可以访问 Internet。

诺顿的调度更新时间可以进行修改，在诺顿杀毒软件窗口的“文件”菜单中选择“调度更新”命令，弹出“调度病毒定义更新”对话框，如图 6-12 所示。

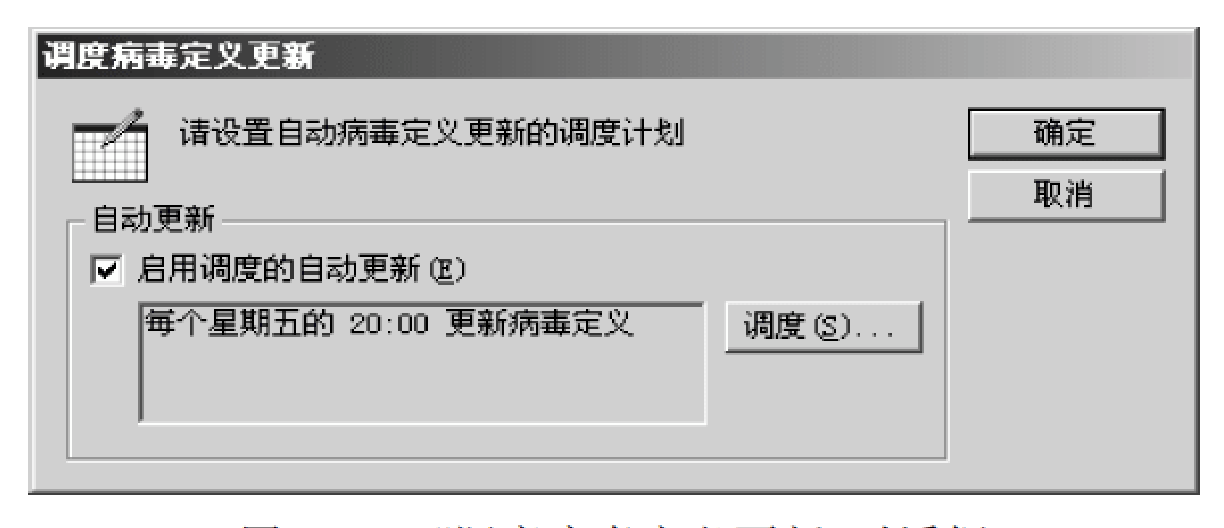


图 6-12　“调度病毒定义更新”对话框

在“调度病毒定义更新”对话框中单击“调度”按钮，可以修改调度更新的时间。

诺顿杀毒软件的调度更新提供了一种方便的更新方式，但是不能保证所有计算机在

 调度更新时都能够连接 Internet，所以有时需要手动更新病毒库。另外当系统报告有新病毒时，不要等到下次调度的更新，而应当立即更新病毒防护。在诺顿杀毒软件窗口中单击 LiveUpdate 按钮，启动手动更新，如图 6-13 所示。



图 6-13　手动更新窗口

单击“下一步”按钮，只要计算机连接到 Internet 并且有新的病毒库，计算机便会进行更新，手动更新进度显示如图 6-14 所示。



图 6-14　手动更新进度显示

病毒库更新完毕单击“下一步”按钮，会显示更新完成，如图 6-15 所示。单击“完成”按钮，诺顿杀毒软件会具有最新的防病毒能力。

2. 使用诺顿杀毒软件扫描计算机

在诺顿杀毒软件窗口的左侧选择“扫描计算机”，然后在右侧列表框中选择需要进行扫描的盘符，如图 6-16 所示。

单击“扫描”按钮，诺顿杀毒软件会对选中磁盘中所有已知的病毒进行查杀，如图 6-17 所示。

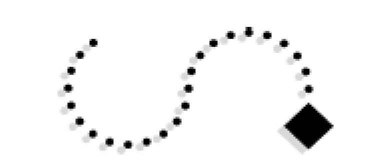




图 6-15　更新完成

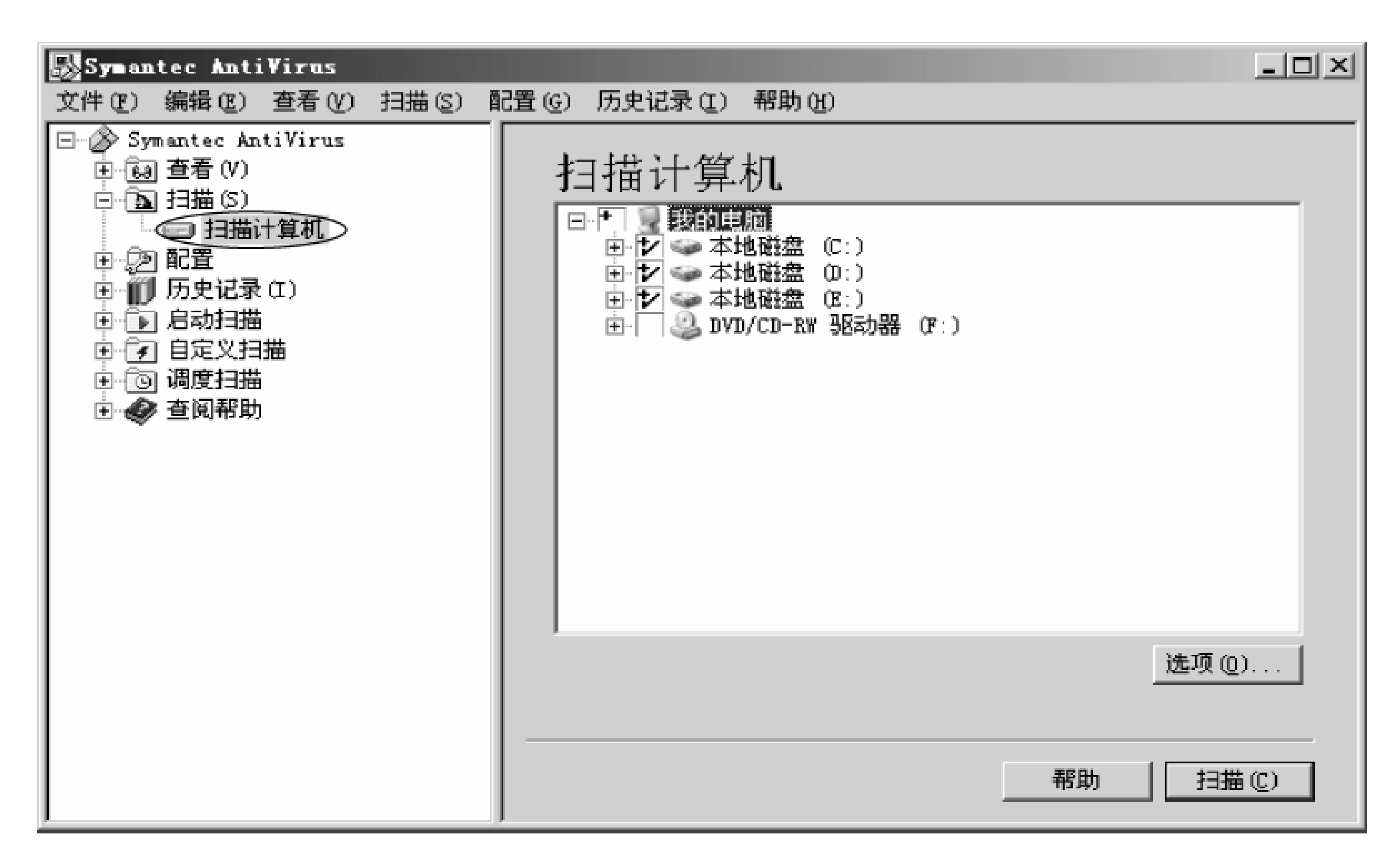


图 6-16　扫描计算机



图 6-17　病毒查杀

在查杀过程中，如果计算机中有病毒，默认情况下系统会弹出一个消息框通知用户，如果病毒比较多，用户就需要不断地关闭消息框，为了避免这种情况发生，可以在图 6-16 中单击“选项”按钮，系统弹出“扫描选项”对话框，如图 6-18 所示。

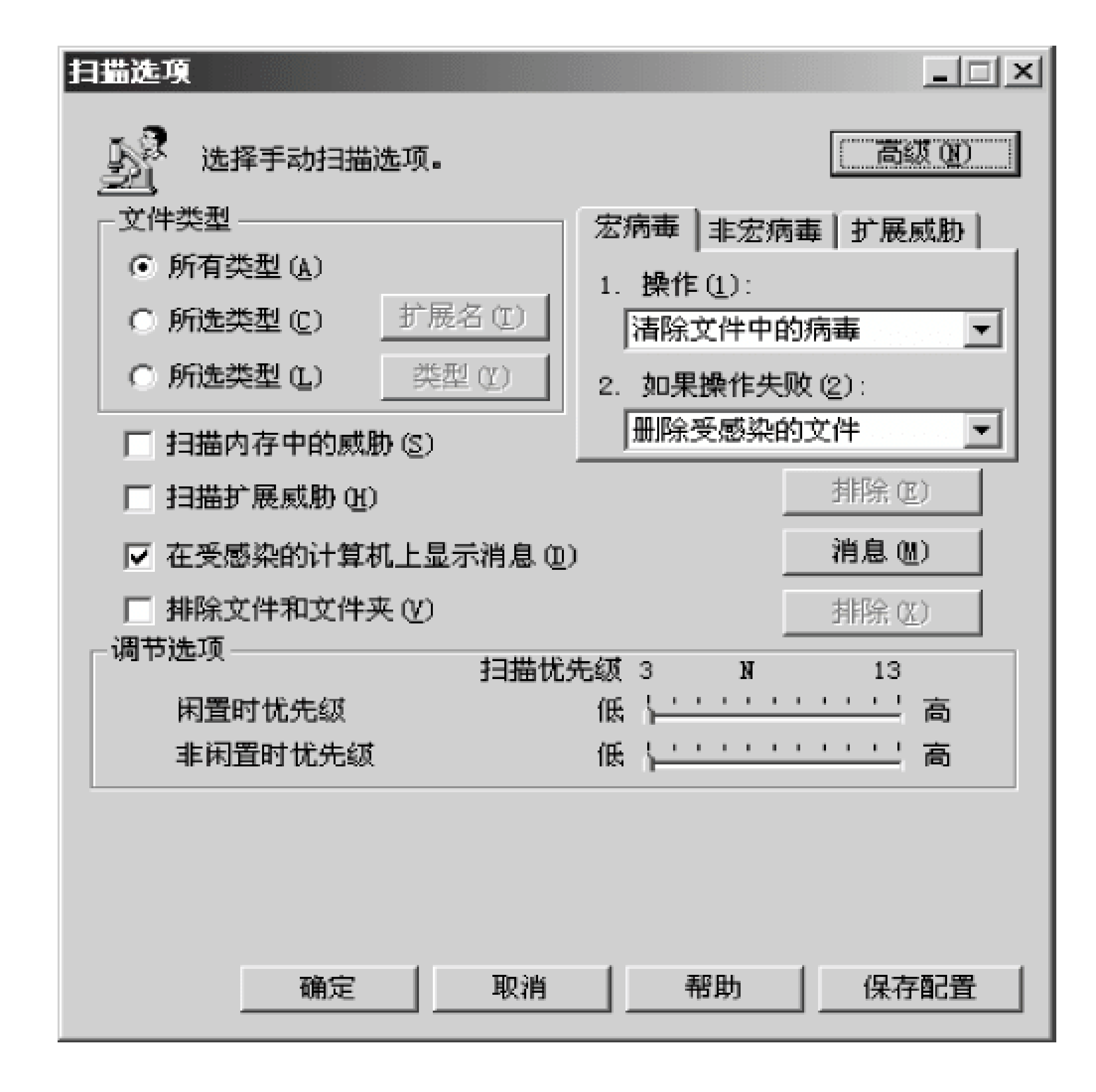


图 6-18 “扫描选项”对话框

在该对话框中将“在受感染的计算机上显示消息(D)”前面的对勾去掉，再单击“确定”按钮对计算机进行扫描，这样在计算机扫描磁盘并发现病毒时就不会弹出消息框。

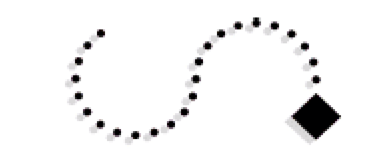
6.2.2 使用卡巴斯基的命令行方式对服务器进行杀毒

网络版的卡巴斯基有两种客户端：工作站版和服务器版。工作站版杀毒软件是不能安装在 Windows Server 操作系统上的，其使用方法和其他杀毒软件的使用方法基本相同。服务器版安装以后，没有图形界面可以进行杀毒操作。如果想对服务器进行杀毒有两种方法，第一种方法是使用网络版的管理服务器进行杀毒操作，另一种方法是使用 DOS 命令进行杀毒操作。

1. 卡巴斯基命令行所支持的命令

使用命令行可以运行卡巴斯基反病毒程序，所支持的命令如下：

SCAN	扫描所选的对象
FULLSCAN	完整的计算机扫描
UPDATE	更新反病毒数据库和应用程序模块
ROLLBACK	恢复到最后一次病毒库更新之前的状态
RTP	实时保护方式管理
START	运行卡巴斯基反病毒程序
STOP	停止卡巴斯基反病毒程序
TASK	管理卡巴斯基反病毒程序任务
CONVERT	报告转换成为容易阅读的格式



2. 使用命令行方式扫描磁盘

使用命令行方式扫描服务器需要在 DOS 窗口中进入卡巴斯基的安装目录，默认安装目录是 C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus for File Servers 5>，在命令提示符下输入 kavshell scan c：d：，其中 c：和 d：为系统盘符。

SCAN 命令有许多参数，其中，DISINFECT 参数可以对扫描过程中发现的病毒进行查杀，DELETE 参数可以对发现的病毒进行删除，但这两个参数不能同时使用，例如，

```
kavshell scan c: d: /disinfect
```

或

```
kavshell scan c: d: /delete
```

3. 使用命令行进行完整扫描

完整的计算机扫描命令是 FULLSCAN，例如，

```
kavshell fullscan
```

也可以将完整扫描后的日志文件存入指定的文档，用于扫描完成后进行查看，例如，

```
kavshell fullscan /WA: fullscan.log
```

4. 使用命令行运行更新

运行更新的命令是 UPDATE，例如，

```
kavshell update
```

默认情况下是更新病毒库和应用程序模块，若只更新应用程序模块可以增加 APP 参数，例如，

```
kavshell update /APP
```

5. 其他命令

卡巴斯基服务器版还有其他命令，在 DOS 提示符下可以使用"?"号查看命令的帮助文档，例如，

```
kavshell /? 或 kavshell scan /?
```

6.2.3　杀毒软件的选择

病毒仍在肆虐全球，它的数目和种类如此之多，而与之针锋相对的杀毒软件也在日新月异地变化。对杀毒软件的选择有时也很让用户头疼，一个好的杀毒软件必须具有以下特点才值得用户使用。

（1）能查杀病毒的数量要多。此外还要求反病毒软件在杀毒时不破坏文件，运行可靠，杀毒时不出现死机现象。

（2）要有实时反病毒的防火墙技术。实时防火墙技术就是时刻监视系统状况，对病毒的传播途径进行严密的封锁，将病毒阻止在操作系统之外。

（3）内存占有量小，恢复数据能力要强。一旦病毒发作，杀毒软件应能迅速修复被破

坏的硬盘分区表,然后恢复分区上的数据。杀毒软件占内存小,意味着不影响其他程序的运行。

(4) 软件有及时的升级服务和良好的售后服务。及时升级就能在最短的时间内对最新的病毒做出反应,保证系统的安全性,良好的售后服务能对客户的合理要求做出正确的回复。

6.3 黑客攻防案例

6.3.1 入侵案例

该案例所攻击的服务器 IP 地址为 192.168.1.2,所使用的第三方软件为 X-Scan v3.2。

1. 获得用户名和密码

黑客在进行攻击的时候最想获得用户名和密码,因为只要获得用户名和密码就可以控制服务器。

X-Scan 软件是安全焦点(http://www.xfocus.org)版权所有的一款漏洞检测软件,通过这个软件可以检测到网络中计算机的用户名和弱口令。X-Scan v3.2 GUI 窗口如图 6-19 所示。

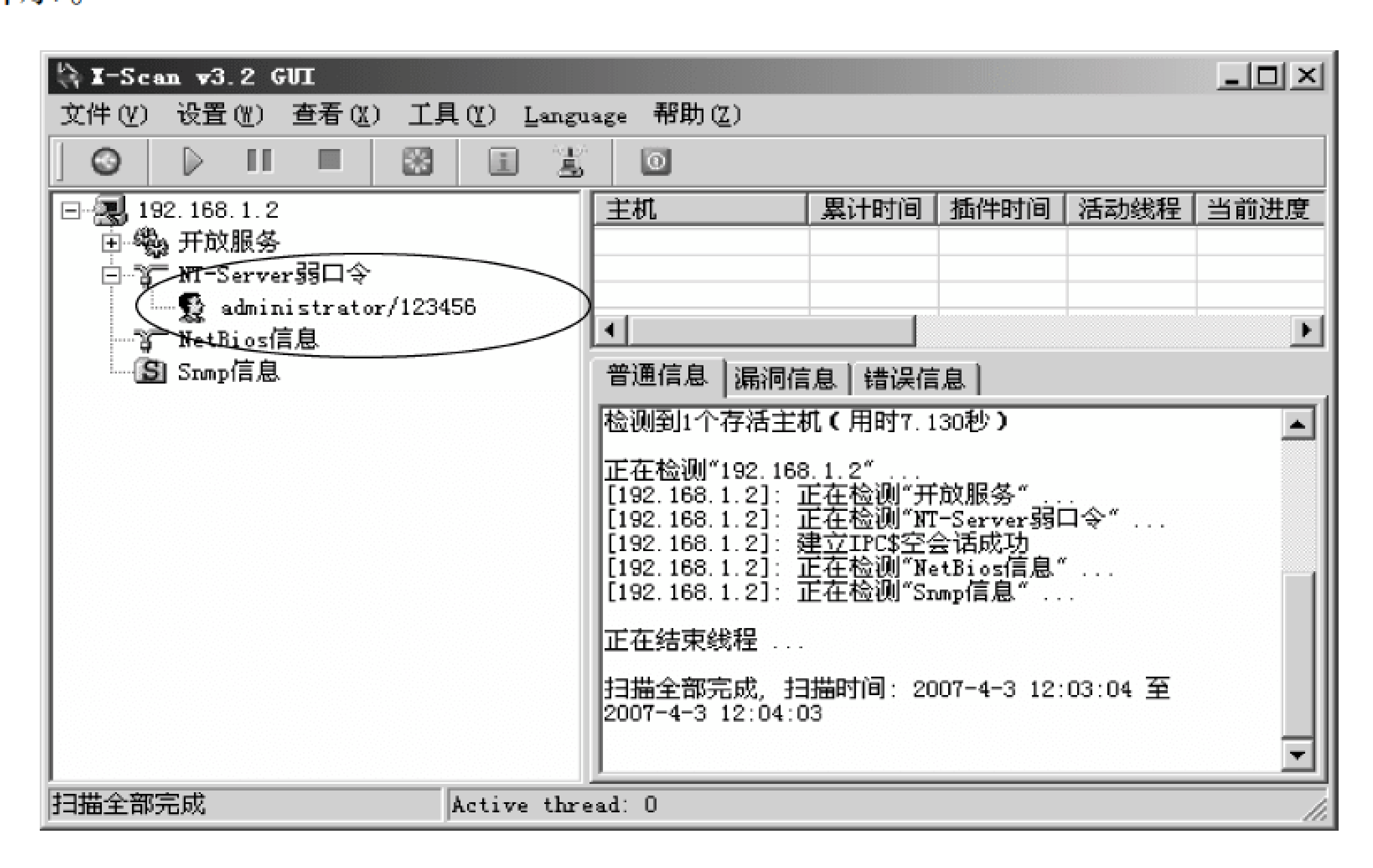


图 6-19 X-Scan v3.2 GUI 窗口

在该窗口中可以看到 X-Scan 检测到 NT-Server 弱口令,所以 192.168.1.2 的用户名为 administrator,密码为 123456。

2. 远程修改注册表

黑客知道了用户名和密码以后,将本机的用户名和密码进行修改,并要和 192.168.1.2 的用户名和密码相同,否则在连接网络注册表系统时会出现错误提示。

在 Windows Server 2003 系统中选择"开始"→"运行"命令,在"运行"对话框中输入 regedit,单击"确定"按钮,打开"注册表编辑器"窗口,如图 6-20 所示。



图 6-20　“注册表编辑器”窗口

在“注册表编辑器”窗口中选择“文件”→“连接网络注册表”命令，打开“选择计算机”对话框，如图 6-21 所示。



图 6-21　“选择计算机”对话框

在“选择计算机”对话框的“输入要选择的对象名称(例如)”文本框中输入 192.168.1.2，单击“确定”按钮，注册表编辑器会连接到远程服务器 192.168.1.2，如图 6-22 所示。

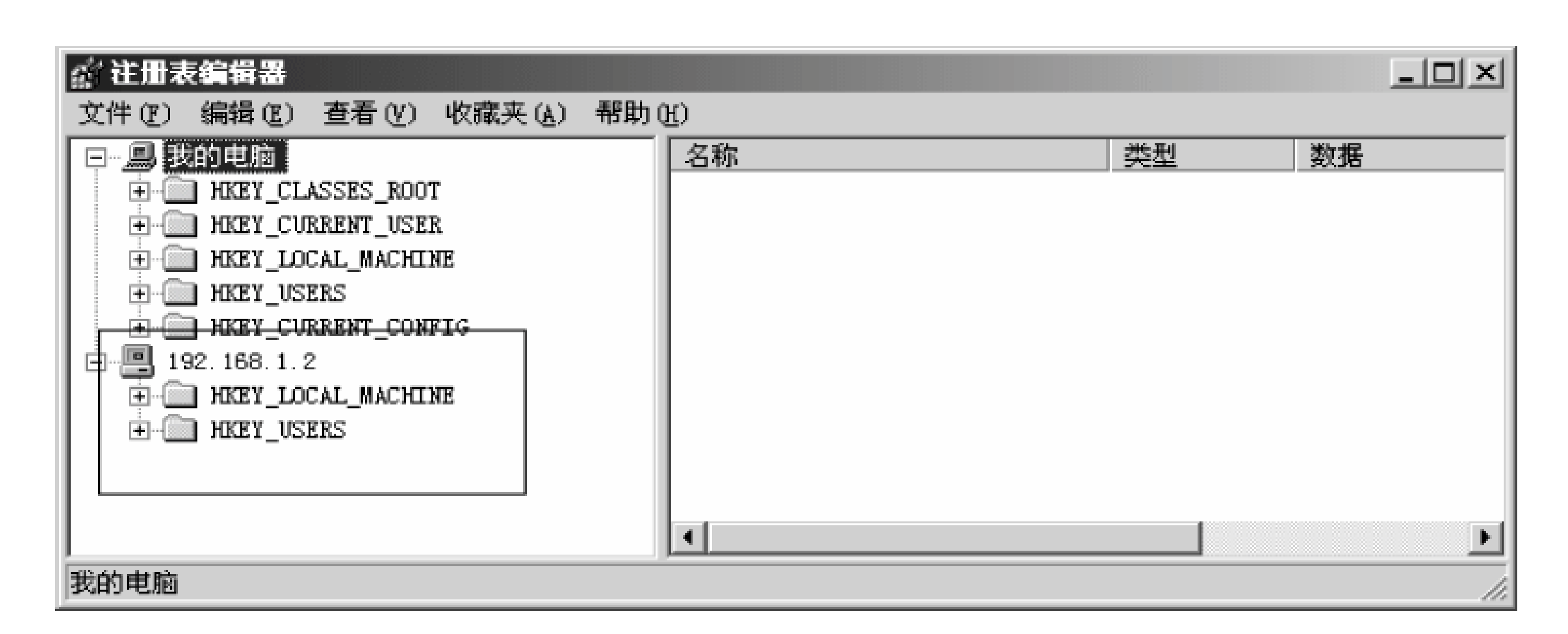


图 6-22　连接到 192.168.1.2

打开 192.168.1.2 的注册表项：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server，将其中 fDenyTSConnections 的键值修改为 0，0 代表启用远程桌面，1 代表禁用远程桌面，如图 6-23 所示。



图 6-23　修改键值

3. 重新启动远程服务器

修改完注册表后，可以使用 shutdown 命令对其重新启动远程服务器：

```
shutdown -m 192.168.1.2 -r
```

4. 远程登录服务器



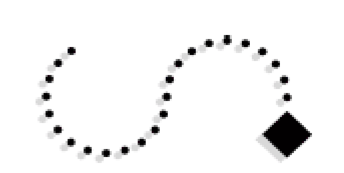
图 6-24　“远程桌面连接”对话框

选择“开始”→“程序”→“附件”→“通讯”→“远程桌面连接”命令，弹出如图 6-24 所示的“远程桌面连接”对话框。

在该对话框中输入远程计算机的 IP 地址 192.168.1.2，单击“连接”按钮，弹出远程桌面的登录界面，如图 6-25 所示。



图 6-25　登录界面



在登录界面中输入用户名 Administrator 和密码 123456，单击“确定”按钮，远程桌面就会登录到 192.168.1.2 的系统中，如图 6-26 所示。



图 6-26　登录成功

成功进入 192.168.1.2 的系统，标志着黑客此次入侵完成。

6.3.2　防御案例

1. 修改 TTL 值防止黑客辨别操作系统

黑客经常会根据对方的操作系统来策划攻击方案，一般是通过 Ping 对方主机所返回的 TTL 值来判断对方的操作系统。不同的操作系统的 TTL 值是不相同的，默认情况下，Linux 系统的 TTL 值为 64 或 255，Windows NT/2000/XP 系统的 TTL 值为 128，Windows 98 系统的 TTL 值为 32，UNIX 主机的 TTL 值为 255。如果将 Windows Server 2003 的 TTL 值修改为 255，那么黑客就会以为这个服务器是 Linux 系统或 UNIX 系统，就会针对 Linux 系统或 UNIX 系统来查找服务器的安全漏洞，但是黑客不会找到服务器的安全漏洞，因为操作系统的类型不一样，这样一来，服务器就安全多了。

只要修改注册表就可以修改 Windows Server 2003 的 TTL 值。选择“开始”→“运行”命令，在“运行”对话框中输入 regedit，单击“确定”按钮，弹出“注册表编辑器”窗口，如图 6-27 所示。

展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\





图 6-27 “注册表编辑器”窗口

Parameters 注册表项，在该项中新建一个名为 defaultTTL 的 DWORD 值，并将该值修改为十进制的 255，如图 6-28 所示。

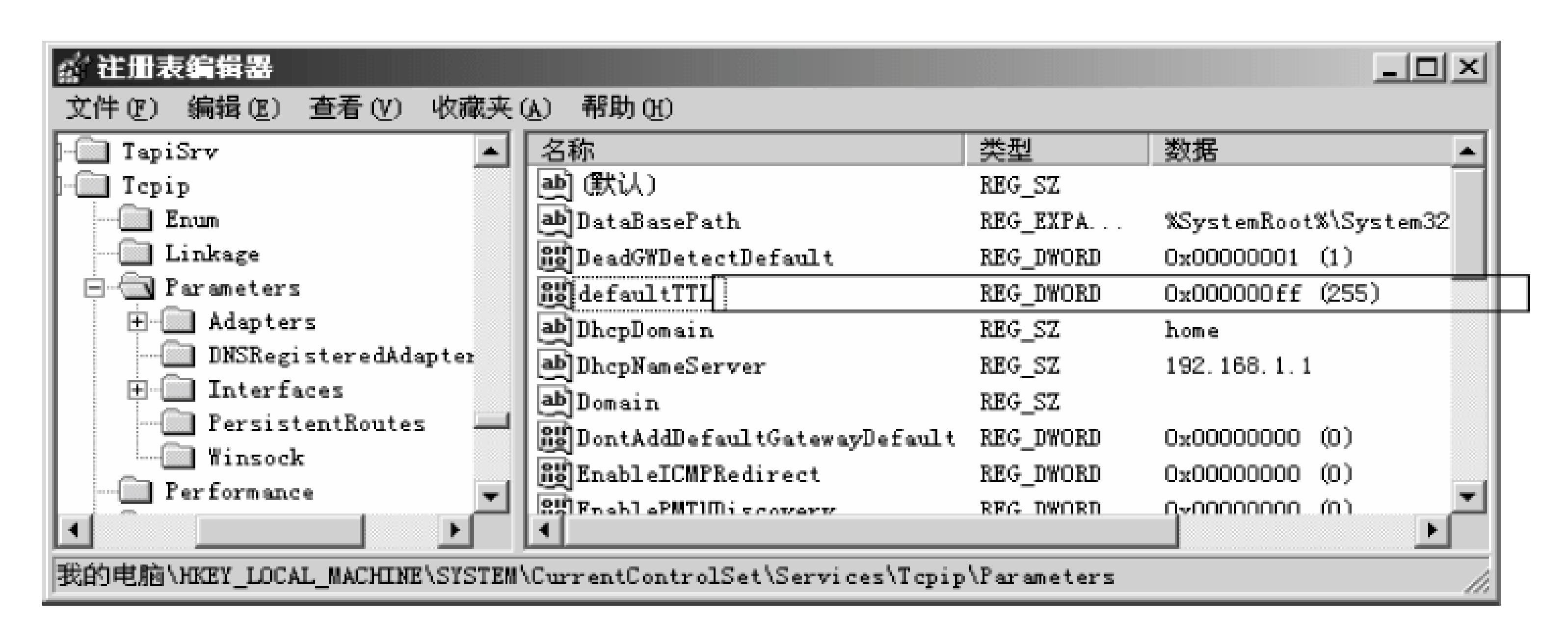


图 6-28 创建 defaultTTL 的 DWORD 值

修改完注册表后服务器需要重新启动，重新启动服务器之后使用 Ping 命令测试服务器的 TTL 值是否为 255，如图 6-29 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>ping 192.168.1.3

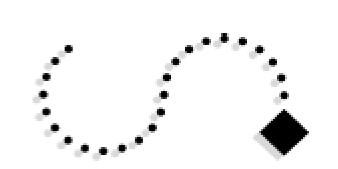
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

图 6-29 测试 TTL 值



2. 查看 FTP 口令是否被暴力破解

FTP 口令对于服务器的管理而言是非常重要的，破解 FTP 口令最常用的方法就是暴力破解，所以系统管理员要经常更换系统密码。

如果想要查看 FTP 口令是否被暴力破解，可以在“控制面板”窗口中单击“管理工具”图标，在“管理工具”窗口中双击“计算机管理”图标，打开“计算机管理”窗口，如图 6-30 所示。



图 6-30　“计算机管理”窗口

在“计算机管理”窗口中单击“事件查看器”→“系统”，如果在系统日志中发现大量时间相同或非常接近、ID 值为 100 的系统警告信息，而且这些警告信息的来源标记为 MSFTPSVC，然后再查看该信息的详细内容，如有类似 “由于以下错误，服务器无法登录到 Windows NT 账号‘xxx’：登录失败：未知的用户名或错误密码。”的信息，就可以断定有人曾经暴力破解 FTP 口令，如图 6-31 所示。

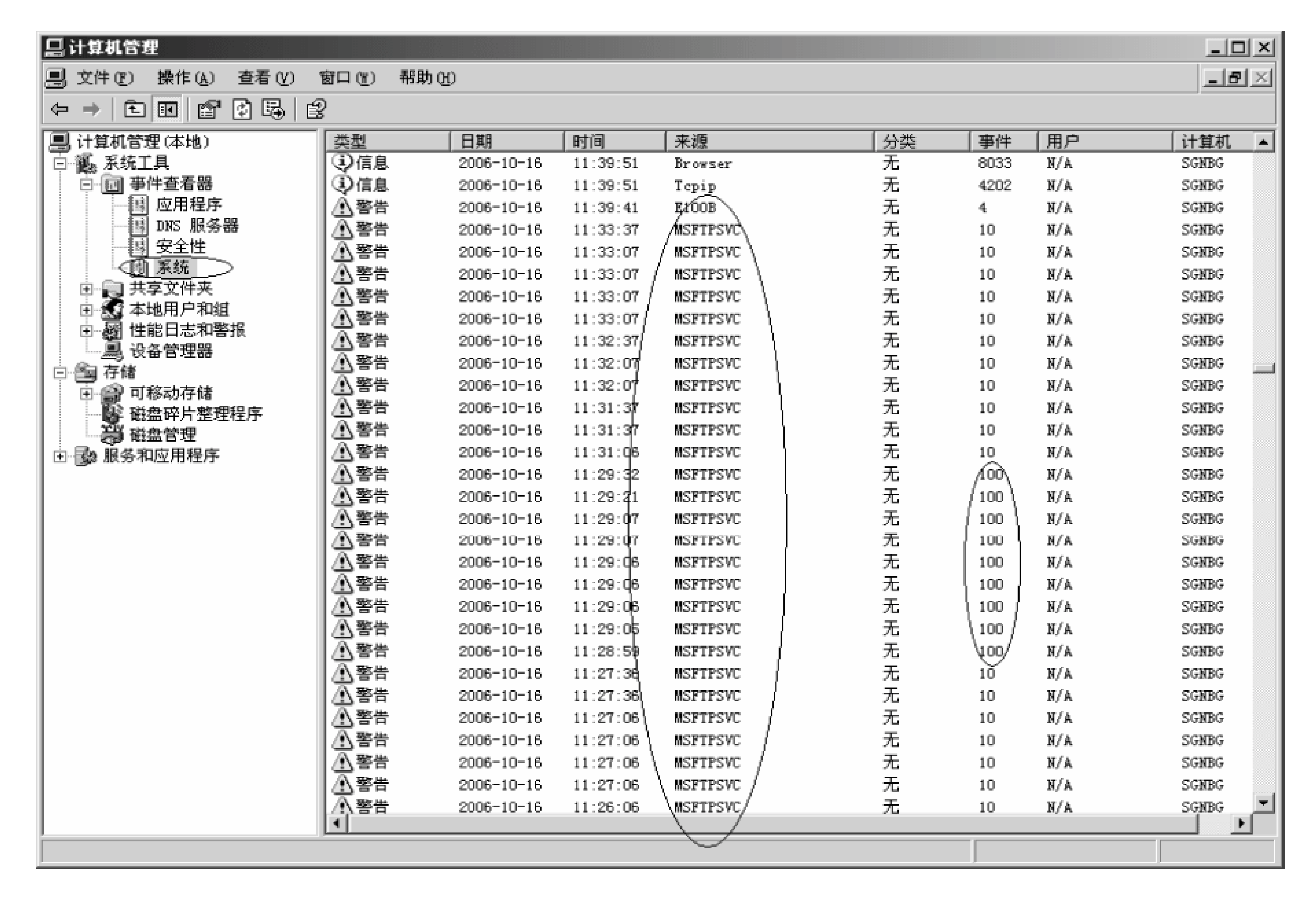


图 6-31　系统日志

发现有人暴力破解 FTP 口令，管理员要做的第一件事就是修改口令，第二件要做的事就是查找攻击来源。

管理员可以通过查看 FTP 站点的日志来查找攻击来源。FTP 站点的日志存放在 C:\WINDOWS\system32\LogFiles\MSFTPSVC1\中，根据暴力破解的时间查看日志，可以发现如下格式的文本：

```
2006-10-16 11:29:36 192.168.1.2 administrator MSFTPSVC1 SGNBG 192.168.1.3 21 [18]USER
administrator - 331 0 0 0 0 FTP - - - -
2006-10-16 11:29:36 192.168.1.2 - MSFTPSVC1 SGNBG 192.168.1.3 21 [18]PASS - - 530 1326 0 0
0 FTP - - - -
```

其中，administrator 为受攻击的用户名，192.168.1.2 为攻击源的 IP 地址，PASS - - 530 1326 0 0 0 FTP - - - -说明登录没有成功。

6.4　设置相对安全的 Windows Server 2003 系统

当今时代是 Internet 的时代，在 Internet 上发布自己的站点对外提供服务已经不是一件难事，但保证服务器安全却是网络管理员最重要的职责之一。网络管理员应设置相对安全的操作系统，用于防御一般性的黑客攻击。

1. 硬件环境

(1) CPU：奔腾 2.0GHz。

(2) 内存：DDR 256Mbps。

(3) 光驱：52X CD-ROM。

(4) 硬盘：80Gbps。

(5) 网卡：100Mbps。

2. 软件环境

(1) 系统软件：Windows Server 2003 中文版。

(2) 应用软件：Serv-U——用于设置 FTP；
SQL Server——用于建立数据库；
Norton AntiVirus——杀毒软件。

(3) 工具软件：WinRAR——用于压缩/解压缩软件；
Ghost——用于进行操作系统的备份。

其中应用软件和工具软件最好使用最高版本。

3. 提供服务

(1) DNS 服务：域名解析。

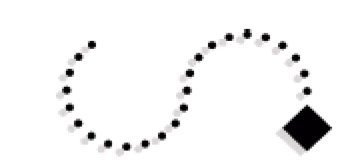
(2) FTP 服务：文件传输。

(3) WWW 服务：网站浏览。

4. 实施步骤

(1) 安装操作系统

操作系统安装是网络管理员的第一步，应根据系统所提供的服务并使用 NTFS 格式



化分区将硬盘分为3个区，即C、D和E，如图6-32所示。

Windows Server 2003, Enterprise Edition 安装程序

以下列表显示这台计算机上的现有磁盘分区
和尚未划分的空间。

用上移和下移箭头键选择列表中的项目。

◎ 要在所选项目上安装 Windows，请按 Enter。

◎ 要在尚未划分的空间中创建磁盘分区，请按 C。

◎ 删除所选磁盘分区，请按 D。

78600MB Disk 0 at Id 0 on bus 0 on symmpi [MBR]
C: 分区 1 [新的(未使用)] 14980MB (14980MB 可用)
D: 分区 2 [新的(未使用)] 49970MB (49970MB 可用)
E: 分区 3 [新的(未使用)] 13642MB (13642MB 可用)
未划分的空间 8 MB

Enter=安装　C=创建磁盘分区　F3=退出

图6-32　硬盘分区

C盘为15Gbps，用于存放系统文件。

D盘为50Gbps，用于存放Web站点文件、FTP站点文件及数据库文件。

E盘为剩余硬盘空间，用于存放服务器的镜像文件、各种软件的安装文件、备份文件及各种日志文件。

(2) 安装杀毒软件

杀毒软件是所有计算机必须装的，包括服务器在内。杀毒软件不但可以为服务器提供最基本的防护，而且还可以防止黑客上传木马程序。因为杀毒软件对计算机是实时检测的，当木马程序准备运行时，杀毒软件会将其杀掉。

(3) 安装应用软件

在安装其他应用软件时可以使用默认安装模式，但在安装SQL Server时要注意以下两点：

① 不要用sa作为数据库的默认用户名，用户名需要进行修改；

② 安装完毕，在建立数据库时要将数据库的存放路径进行修改，如图6-33所示。

(4) 安装补丁或升级

在没有安装杀毒软件之前尽量不要上网在线更新补丁，如有条件可以通过其他计算机下载补丁数据包，然后再进行更新。现在Windows Server 2003中文版已经有SP1补丁，SQL Server已经有SP3补丁。

补丁包安装完毕再上网更新杀毒软件的病毒库，病毒库一定要更新到最新为止；最后到微软网站察看是否有最近的更新，直到IE浏览器显示“安装更新程序(0)。”为止，微软系统更新页面如图6-34所示。

(5) 禁用Guest账号

Guest账户即来宾账户，该账户可以访问计算机，但会受到限制。而且Guest用户也会被黑客利用，所以禁用或删除Guest账户是最好的办法。

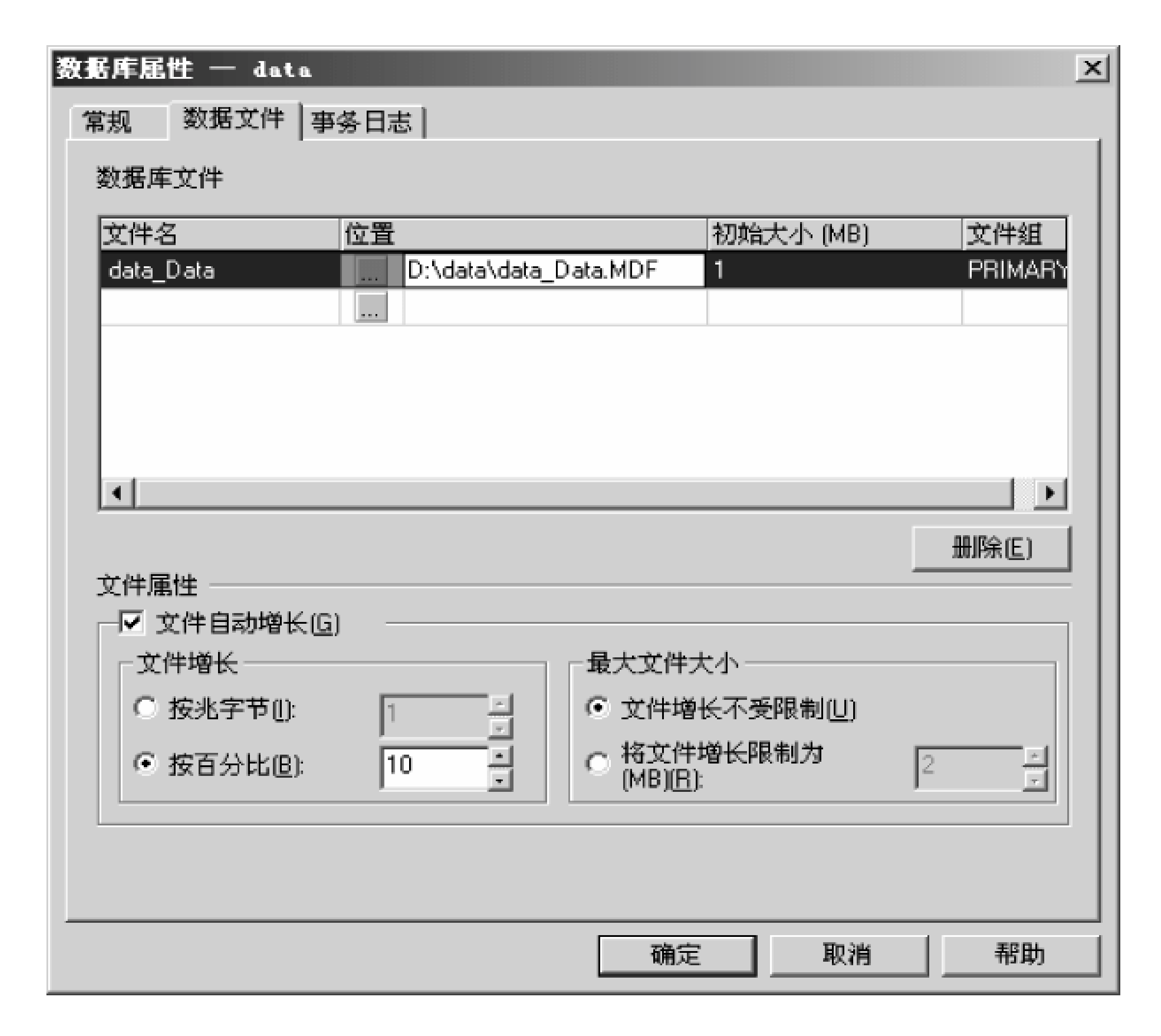


图 6-33　修改数据库路径

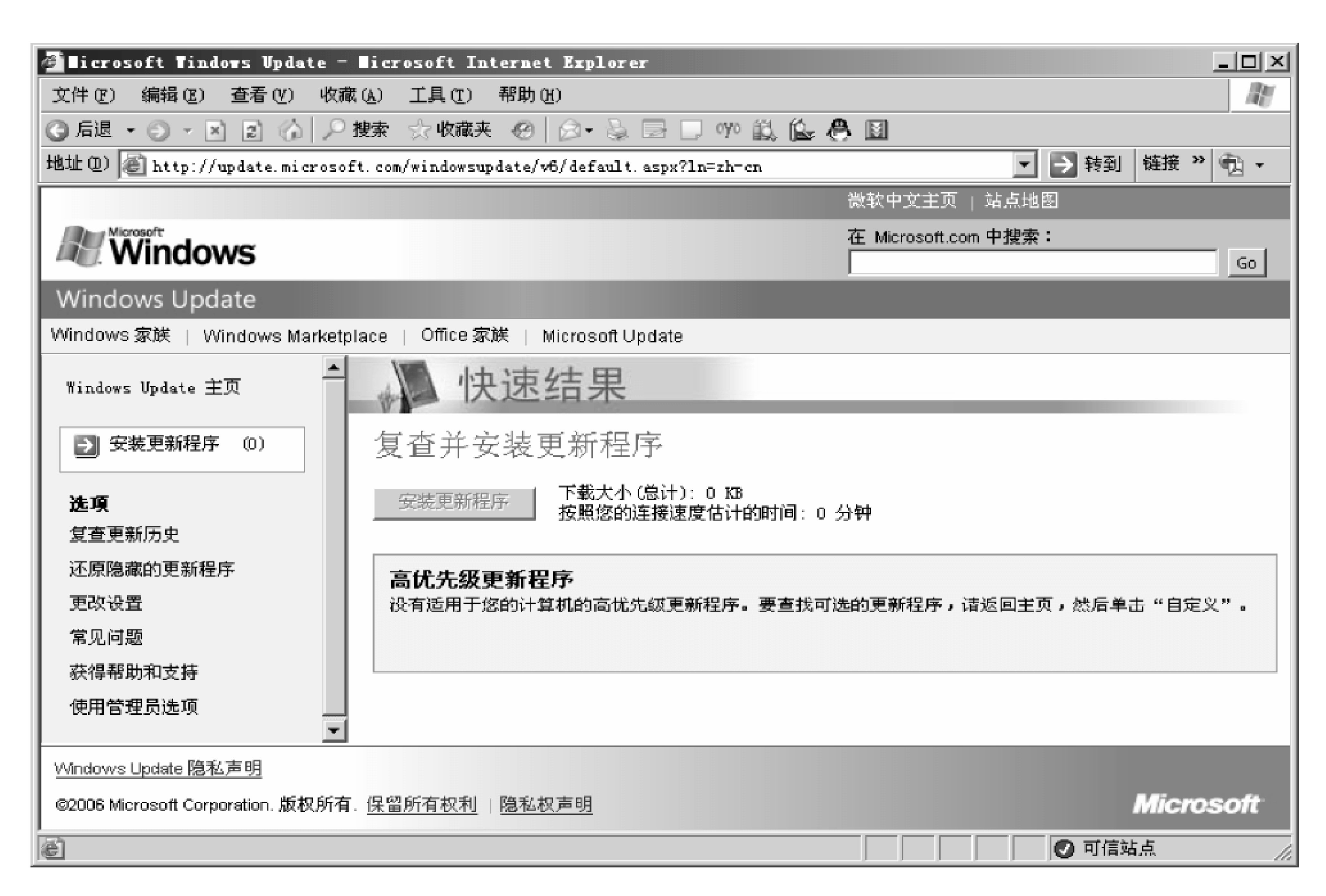


图 6-34　微软系统更新页面

(6) 更改超级用户名并设置密码

几乎所有的黑客都知道 Windows Server 2003 的超级用户是 Administrator，只要知道了超级用户的密码便可以畅通无阻了，所以管理员不但要为超级用户设置一个复杂密码，而且要更改超级用户的用户名。如果有必要可以再建立一个名为 Administrator 的陷阱用户，并且使用复杂的字符串作为密码，然后让该用户不具有任何权限，这样就算黑客费尽周折破解了这个用户的密码，也不能对服务器进行攻击。在图 6-35 中，Administrator 为陷阱用户，而真正的超级用户名为 sgnrn。

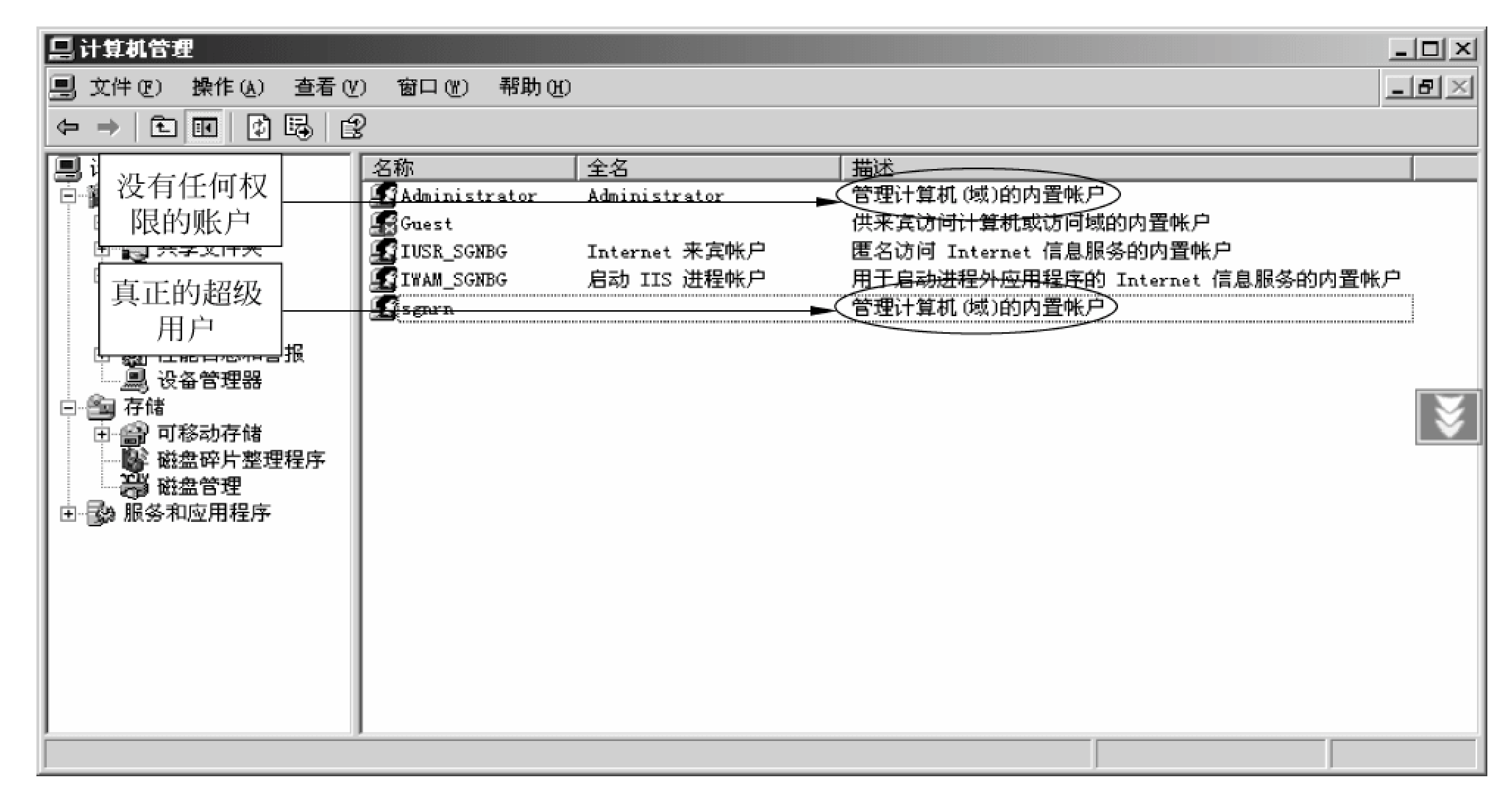


图 6-35　设置超级用户

(7) 设置用户访问权限

有些文件不是所有用户都需要访问的，即使需要访问也不一定需要所有的权限，所以设置用户的访问权限只有一个原则，就是只开放用户所需要的权限，其他权限一律关闭。在设置用户权限时，首先将所有磁盘设置为只允许超级用户访问，并开放所有权限，其他用户均删除。由于 D 盘需要存放 Web 站点文件、FTP 站点文件及数据库文件，应该允许其他用户浏览，但并不要求其具有写或更改的权限，所以可以设置 Everyone 用户对 D 盘具有“读取和运行”、“列出文件夹目录”和“读取”权限，如图 6-36 所示。

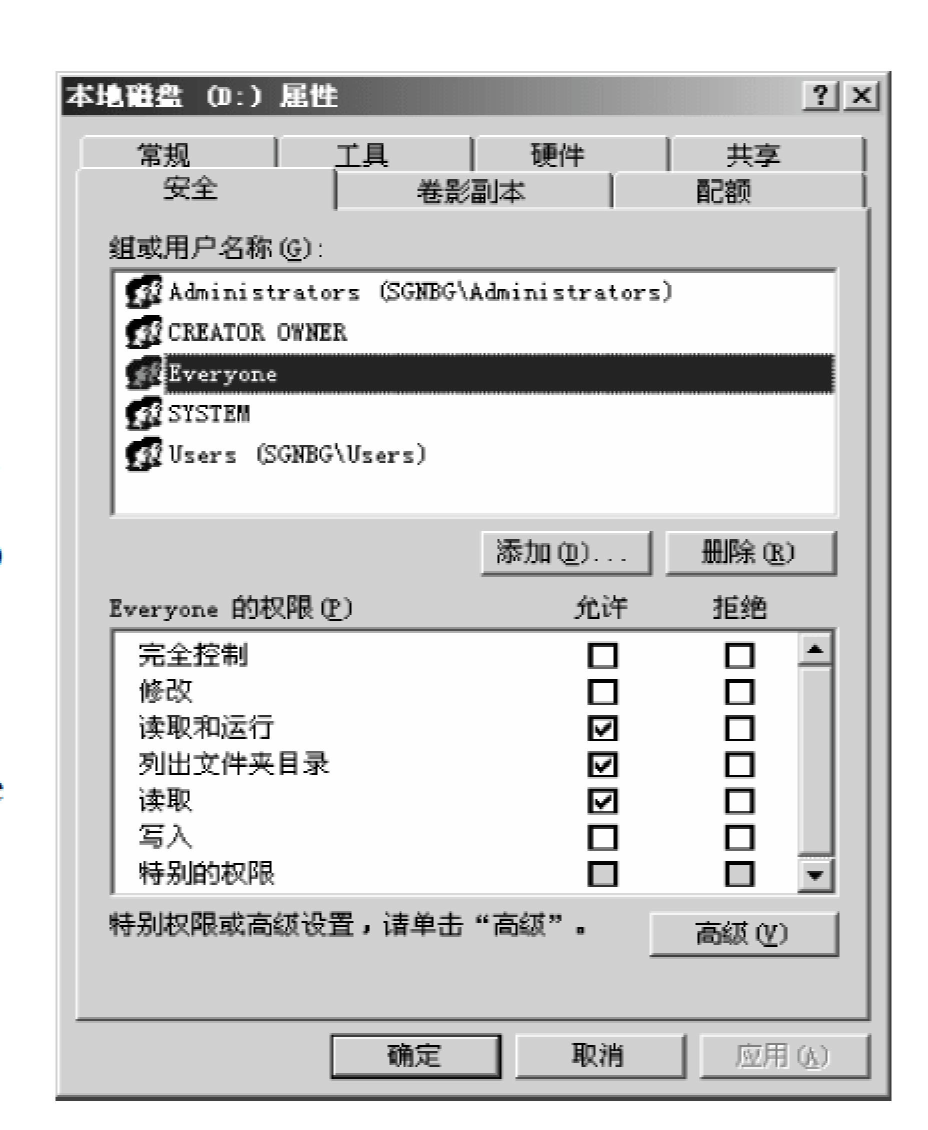


图 6-36　设置用户访问权限

用户访问权限的设置可以有效地抑制黑客入侵，如果服务器还需要设置其他特殊用户或权限，可以另行设置。

（8）禁用不使用的服务

在进行服务器配置的时候，有一些服务是没有必要的，在特定的情况下这些服务有可能会变成黑客可利用的工具。“服务”控制台可以让用户关闭不需要的服务。在“控制面板”中双击“管理工具”图标打开“管理工具”窗口，在“管理工具”窗口中双击“服务”图标打开“服务”窗口，该窗口显示了服务器所运行的所有服务，如图 6-37 所示。

名称	描述	状态	启动类型	登录为
Adobe LM Service	Ado...		手动	本地系统
Alerter	通...		禁用	本地服务
Application Ex...	在...	已启动	自动	本地系统
Application La...	为...	已启动	手动	本地服务
Application Ma...	为 ...		手动	本地系统
Automatic Updates	允...	已启动	自动	本地系统
Background Int...	利...		手动	本地系统
ClipBook	启...		禁用	本地系统
COM+ Event System	支...	已启动	自动	本地系统
COM+ System Ap...	管...		手动	本地系统
Computer Browser	维...	已启动	自动	本地系统
Cryptographic ...	提...	已启动	自动	本地系统
DCOM Server Pr...	为 ...	已启动	自动	本地系统
DHCP Client	为...	已启动	自动	网络服务
DHCP Server	为 ...	已启动	自动	本地系统
Distributed Fi...	将...		手动	本地系统
Distributed Li...	启...	已启动	自动	本地系统
Distributed Li...	启...		禁用	本地系统
Distributed Tr...	协...	已启动	自动	网络服务

图 6-37 “服务”窗口

以下是建议禁用的服务：

Computer Browser：维护网络计算机更新，禁用。

Distributed File System：局域网管理共享文件，不需要可禁用。

Distributed Link Tracking Client：用于局域网更新连接信息，不需要可禁用。

Error Reporting Service：发送错误报告，不需要可禁用。

Microsoft Search：提供快速的单词搜索，不需要可禁用。

NT LM Security Support Provider：Telnet 服务所使用的，不需要可禁用。

Print Spooler：打印服务，如果没有打印机可禁用。

Remote Registry：远程修改注册表，不需要可禁用。

Remote Desktop Help Session Manager：远程协助，不需要可禁用。

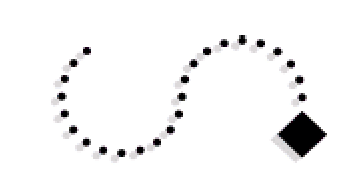
（9）设置 IIS 服务

不使用默认的 Web 站点建立 Web 服务，可以在 IIS 中重新建立一个 Web 站点，并将默认的 Web 站点删除。

删除 IIS 默认创建的 Inetpub 目录，因为该目录具有安全隐患。

（10）修改日志文件目录

尽量修改所有日志文件的默认目录，以防止黑客恶意删除日志文件，另外有些日志文件可以在被攻击以后用来分析攻击源或攻击手段。



（11）设置 FTP 服务

FTP 服务可以使用 IIS 中所提供的 FTP 功能，也可以使用 Serv-U，但是要使用最新版本，因为低版本的 Serv-U 软件有漏洞，最新版本会好一些。

（12）系统备份

在 C 盘制作一个 GHOST 备份，并将镜像文件存放在 E 盘中，以备将来系统崩溃时可以迅速恢复系统，注意，在恢复系统之前，要将日志文件提取出来，用来分析系统崩溃原因。

（13）其他备份

除了系统备份以外，还要将所有的应用软件和驱动程序进行备份，这些备份均存放在 E 盘下，以备不时之需。

5. 总结

在系统设置过程中，每修改一次设置就需要进行一次系统测试，测试内容为服务器对外提供的全部服务。如果所有设置都完毕再进行系统测试，假设有些服务不能够成功访问，将不能确定是哪些设置导致服务访问错误。

6.5　本章小结

本章以案例的形式对第 5 章所讲的理论知识进行了实践性教学环节的训练。通过学习，掌握了服务器操作系统、防火墙及防病毒等软件的安装、配置、使用、升级的方法与技巧；学会了通过对相关软件的设置的修改，加强网络的安全性；了解了黑客进攻的实际过程，希望读者能在此基础上举一反三、触类旁通，能够使用更多的软、硬件产品，来完成增强计算机网络安全的任务。

通过本章学习可以看出黑客攻击并不是很难，只是由于管理员的疏忽；防御也比较容易，只要管理员能够细心使用系统。所以作为一名管理员第一要细心，第二要提高安全意识。

6.6　本章习题

1. 安装瑞星网络版的杀毒软件，并进行服务器端、客户端的相关设置。
2. 在一台计算机上安装天网防火墙，并进行相关设置。
3. 在局域网上，以 X-Scan 软件为工具登录其他的计算机，并在上面建一个名为 123 的文件夹。

第7章

基于 SNMP 协议的管理

本章内容：

本章主要介绍简单网络管理协议 SNMP。SNMP 是一个网络管理的标准，许多网管系统都是基于 SNMP 建立的，一般用于比较复杂的网络环境。与网络操作系统对网络进行管理相比，SNMP 更关注网络中的通信设备和通信层面的状况。

本章重点：

① 掌握网络管理的基本概念。

② 理解管理信息库的基本知识和 SNMP 的协议单元格式及操作。

③ 了解远程网络监控的知识。

如果学时较少，可只学习 7.1 节和第 8 章，有关 SNMP 的内容可不进行学习。

计算机网络最初发展时，网络设备的数目很少，网络管理员只需要 Ping 每台计算机，并通过自动返回的信息就可以判断网络是否出了故障。当计算机网络向全球蔓延，并最终形成全球化的 Internet 时，有成千上百家网络设备厂商生产出几万种不同的网络设备，计算机网络的管理成了巨大的难题，如何对网络进行有效的管理便成为本章研究的问题。

7.1　网络管理的概念

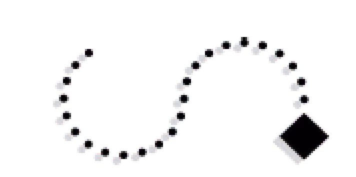
7.1.1　网络管理的内容

根据国际标准化组织（ISO）的定义，网络管理是指规划、监督、控制网络资源的使用和网络的各种活动，使网络的性能达到最优。

1. 网络管理的功能

根据 ISO 定义的网络管理有 5 大功能：配置管理、故障管理、性能管理、计费管理和安全管理。

（1）配置管理。配置管理就是定义、收集、监控和管理系统的配置参数，以使网络性能达到最优。在一个实际的网络系统中网络设备往往是由多个生产厂商提供的，为了使



设备之间可以正确、有效地通信，必须对这些设备进行参数的配置；当网络系统随着工作需要而增减设备时，要对网络的结构进行配置调整；除此之外有些设备（比如防火墙、路由器等）为了满足工作需要，也要进行配置。配置管理根据获取手段大致可以分成 3 类：第一类是根据网络管理协议标准的管理信息库中定义的配置信息进行配置；第二类虽然不在网络管理协议标准中定义，但对设备运行比较重要的配置信息也要进行配置；第三类就是用于管理的一些辅助信息，包括自动备份及相关技术、配置一致性检查和用户操作记录等功能。

（2）故障管理。故障管理是网络管理中最基本的功能，通过采集、分析网络对象的性能数据和监测网络对象的性能，并对网络线路的质量进行分析，最终找出故障的位置并进行恢复的管理操作。其目标是自动监测、记录网络故障并通知网络管理员，以便网络正确、有效地运行。一个网络系统由很多电气设备组成，这些设备由于灰尘、静电、老化或人为的错误操作等问题，都有可能出现各种各样的故障，影响网络的正常运行，这就需要网络故障管理系统。在实际的应用中，网络故障管理包括检测故障、判断故障、隔离故障、修复故障和记录故障等步骤。

（3）性能管理。性能管理主要考察网络运行的好坏，通过收集、监视和统计网络运行的参数数据，例如，网络的吞吐率、用户的响应时间和线路的利用率等，评价网络资源的运行状况和通信效率等系统性能，分析各系统之间的通信操作的趋势，平衡系统之间的负载。性能管理一般包括：收集网络管理者感兴趣的性能参数；分析相应统计数据，以判断网络是否处于正常水平；为每个重要的变量确定一个适合的性能阈值，如果超过该阈值就意味着网络出现故障。

（4）计费管理。计费管理负责记录网络资源的使用情况和使用这些资源的代价。网络中的许多资源都是有偿使用的，计费管理系统就是为了能够统计各个用户使用资源的情况，计算用户应付的费用，控制用户占用和使用过多的网络资源而设计的。计费管理的目标是衡量网络的利用率，以便一个或一组用户可以按规则利用网络资源，这样的规则使网络故障降低到最小（因为网络资源可以根据其能力的大小而合理地分配），也可使所有用户对网络的访问更加公平。为了实现合理的计费，计费管理必须和性能管理相结合。

（5）安全管理。网络系统的安全性是非常脆弱的，为了保障其安全性，需要用户认证、访问控制、数据加密和完整性机制等技术结合使用，来控制用户对网络资源的访问，以保证网络不被有意识的或无意识的侵害，并保证重要信息不被未授权的用户访问。网络安全管理主要包括：授权管理、访问控制管理、安全检查跟踪和事件处理以及密钥管理。

2. 网络管理标准

网络设备的异构性导致网络管理标准化的需求。在网络构建过程中，大量不同型号、不同生产厂家的设备要混合使用，不同类型的网络之间要互相连通，这就需要网络管理系统提供一个统一的、全面的接口，并达到以下目标：

- 具有统一的协议和服务，使管理信息可以保持一致性。
- 对网络性能、安全、配置、计费和故障等方面有标准的定义。
- 允许增加新的应用与服务。
- 减少不同系统之间交换信息的费用。

1979年，ISO开始对网络管理的标准化进行研究，随后国际电报电话咨询委员会也参与了这项研究。1989年ISO颁布了ISO DIS7498-4(X.700)文件，其定义了网络管理的基本概念和总体框架。1991年，ISO又颁布了公共管理信息服务CMIS(ISO 9595)和公共管理信息协议(Common Management Information Protocal，CMIP)(ISO 9596)。CMIP是在TCP/IP的SNMP的基础之上设计的。CMIP采用了面向对象的技术，不仅有数值属性，而且有行为属性，是一种真正的面向对象的技术。但是相对于SNMP而言，CMIP的实现需要大量资源，因此CMIP没能流行起来。1992年ISO公布了系统管理功能SMFs(ISO 10164)和管理信息结构SMI(ISO 10165)，这些文件共同组成了ISO的网络管理标准。虽然ISO制定的标准非常强大，但也非常复杂，因此目前有关ISO管理的实现非常缓慢。

随着因特网的迅速发展，有关TCP/IP网络管理的研究活动十分活跃，相关的网络管理标准也被广泛应用，成为实事上的标准。TCP/IP网络管理标准称为简单网络管理协议(SNMP)，其公布在1990年和1991年的几个RFC文件中，即RFC 1155(SMI)、RFC 1157(SNMP)、RFC 1212(MIB定义)、RFC 1213(MIB-2规范)。由于SNMPv1过于简单，造成系统不够安全和管理上的不完善。几年后产生了简单网络管理协议第二版(SNMPv2)，其定义在RFC 1902～RFC 1908文档中。SNMPv2组合了RMON等内容，使得SNMP在安全和性能方面都有了提高。

除了上述两个网络管理标准外，还有IEEE定义了局域网(LAN/MAN)的管理标准IEEE 802.1b，以及ITU-T为了适应电信网络管理的需要在1989年定义的电信网络管理标准TMN(即M.30建议蓝皮书)等。

7.1.2 网络管理的体系结构

1. 网络管理体系结构的基本概念

对网络管理的能力进行抽象，人们提出了网络管理体系结构的概念。用于定义网络管理系统的结构及系统成员间相互关系的一套规则就是网络管理体系结构。根据网络管理体系结构的定义可知，网络管理体系结构需要研究单个网络管理系统内部的结构及其成员之间的关系，以及研究多个网络管理系统如何相互兼容并连接构成可以管理复杂网络的管理系统。在网络管理体系结构中，网络管理被抽象成一种独特的网络应用。

网络管理体系结构是工作在协议的上层，这是网络管理应用工作的基础结构。网络管理体系结构的特点是：

- 管理功能分为管理站(Manager)和代理(Agent)两部分。
- 为存储管理信息提供关系数据库或面向对象的数据库支持。
- 提供用户接口和用户视图，I和管理信息浏览器等。
- 提供基本的管理操作，如获取管理信息、设置参数以及错误警告等操作。

网络管理体系结构示意图如图7-1所示。

2. TCP/IP网络管理体系结构

早在1987年SNMP就被制订出来，而且不断有新的协议推出，但是SNMP凭借其结构简单、使用方便，且与TCP/IP协议联系紧密的特点一直到今天仍然被广泛地使用。



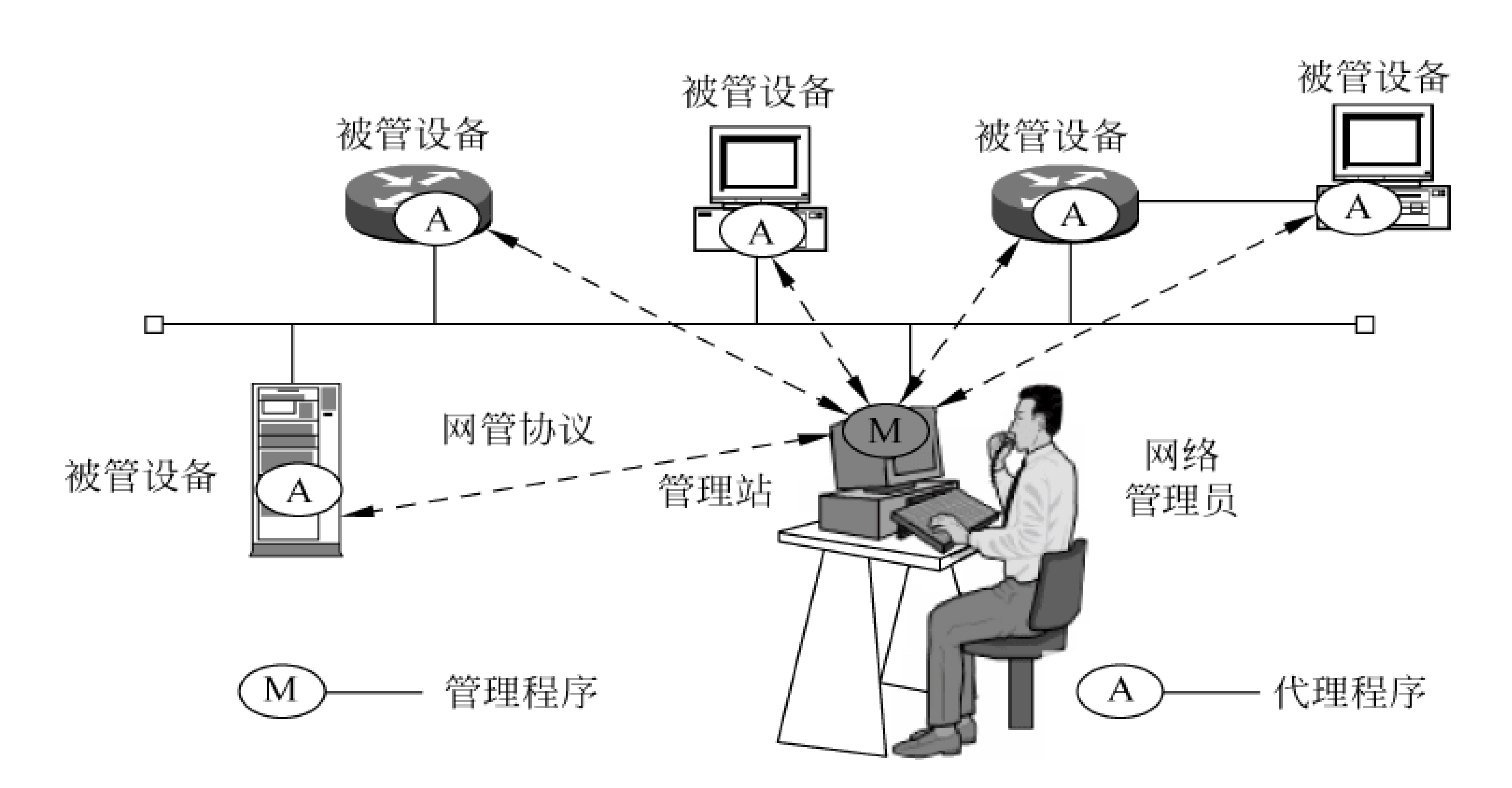


图 7-1　网络管理体系结构示意图

SNMP 管理体系结构由管理者（Manager）、代理（Agent）和管理信息库（MIB）3 部分组成。

管理者是管理指令的发出者，这些指令包括查询和设置参数等管理操作。管理者通过各设备的管理代理对网络内的各种设备、设施和资源实施监控。

代理负责管理指令的执行，并根据结果返回给管理者一些信息。代理有 3 个基本功能。

- 从 MIB 中读取各种变量值。
- 根据管理者的要求修改 MIB 中的各种变量值。
- 当代理设备出现问题时，以通知的形式向管理者报告被管对象发生的一些重要事件。

管理者和代理之间主要以请求/应答方式工作。管理者向代理发出请求指令，获取或者设置网络元素的参数。代理向管理员返回应答响应，报告请求的执行结果。为了使一个管理员可以管理多个代理，常采用轮询的方式。

MIB 是被管对象结构化组织的一种抽象。MIB 是一个概念上的数据库，由管理对象组成，各个代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。

SNMP 是一个异步的请求/响应协议，其实体不需要在发出请求后等待响应的到来。SNMP 中包括了 5 种基本的操作：

- get-request 操作用来查询指定的网络管理对象的信息。
- get-next-request 操作用来查询指定的网络管理对象的下一个对象的信息，该操作还可以遍历 MIB 树并判断哪些对象存在。
- set-request 操作用来修改或创建管理对象及其信息。
- get-response 操作是由代理方发出，所以它不是管理操作，它的作用是返回由 get、get-next 或 set 操作发出的查询或设置操作的结果。
- trap 操作也是由代理发出的，可以查找特定的事件并检测，并向管理者通报重要事件的发生。

SNMP 在计算机网络系统中应用非常广泛，已经成为事实上的计算机网络管理的标准。但是 SNMP 有许多自身难以克服的缺点。

- SNMP 协议的最大问题是太过简单而无法处理各种细节信息，无法满足当今日益膨胀的网络的发展需要，这也是 SNMPv2 以及 SNMPv3 出现的原因。
- SNMP 不适合大型网络管理，因为 SNMP 是基于轮询机制的，这种方式有严重的性能问题，比如不适合查询大量的数据。
- SNMP 协议存在一些安全管理漏洞，网络入侵者很容易获取通过网络传递的各种信息，甚至可以关闭某些终端。
- SNMP 的 trap 是无法确认的，不能确保管理者是否接收到了非常严重的警告信息。
- SNMP 不支持如创建、删除等类型的操作，要完成这些操作，必须用 set 命令间接地触发。
- SNMP 的 MIB 模型不适合比较复杂的查询，因此没有一个标准或建议定义了 SNMP 网络管理体系结构。另外，由于定义了太多的管理对象类，当管理者需要查询或修改时，他必须明白这些管理对象类的准确含义。

7.2 管理信息库

管理信息库(Management Information Base，MIB)是一个以层次式树型结构为组织结构的管理信息的集合，所有的管理对象都分布在这个树型结构中。MIB 被 SNMP 协议访问和使用。

7.2.1 管理信息结构

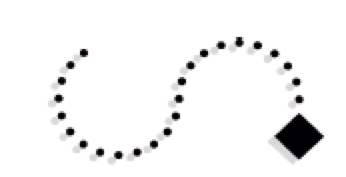
管理信息结构(Structure of Management Information，简称 SMI)，为命名和定义管理对象指定了一套规则。上百家网络设备厂商的产品都遵循这个规则，以使网络设备能够相互兼容。

1. ASN.1 简介

ASN.1 是 Abstract Syntax Notation One(抽象语法符号 1)的简称，是一种标准的对象定义语言和编码规则。虽然 ASN.1 太复杂、缺点多、运算效率不高，但是 SNMP 已经完全溶进 ASN.1 了，所以要想了解 SNMP，就必须熟悉 ASN.1。

在 SNMP 上应用的 ASN.1 有一些用词上的惯例：

- 固有的数据类型一般都以大写字母表示，比如 OCTET STRING。
- 用户自定义的数据类型以大写字母开头，但至少有一个非大写字母，以便与固有的数据类型区分开。
- 标识符可以包括大写字母、小写字母、数字和下划线，但必须以小写字母开头，比如 internet。
- 空格、回车符和 Tab 键并不十分重要。
- 注释以字符串“--”开头，直到行尾或下一个字符串“--”出现。



ASN.1 一共有 5 种固有的基本数据类型，表 7-1 所示为在 SNMP 中使用的 ASN.1 的基本数据类型和其说明。

表 7-1　在 SNMP 中使用的 ASN.1 的基本数据类型及其说明

基本数据类型	说　明
INTEGER	任意长度的整型数
BIT STRING	一个 0 或多位比特的串
OCTET STRING	一个 0 或多位无符号字节串
NULL	位置符，表示为空
OBJECT IDENTIFIER	对象标识符类型

理论上没有规定 INTEGER 类型的长度范围，但是其他的 SNMP 规则限制了它的范围，因为实际应用中不可能出现无限大这种情况。下面列举一个使用 INTEGER 类型的例子，用 ASN.1 定义了一个 INTEGER 类型的变量 counter 并初始化为 1。

示例如下：

```
counter INTEGER::=1
```

有时也需要一种整型的子类型，将变量的值限定为特定的一些值或在一定的范围内，实际应用中这种情况较常见。例如，定义一个状态子类型 Status，其定义如下：

```
Status::=INTEGER{up(1),down(2),unknown(3)}
```

定义好后，就可以应用这种子类型了。例如，接口 1(interface1)的定义。

示例如下：

```
Interface1 Status::=1
```

BIT STRING 是比特串，其每一个比特要不是 0，要不是 1。与其相似的是 OCTET STRING(无符号字节串)类型，只不过这种类型中每一个字节的范围是从 0～255。上述两种类型，可定义串的长度和初值。

NULL 表示空，或是位置符。例如，在 SNMP 的 get 操作中的对象标识符值域中就是 NULL 类型。

OBJECT IDENTIFIER 是一种标识管理对象的方法，这些管理对象被组织成一种树的结构存放，从树的“根”开始到每一个管理对象都有惟一的一条路径，相应地也就有惟一一个标识。例如，定义 internet 的对象标识符。

示例如下：

```
Internet OBJECT IDENTIFIER::={iso(1) org(3) dod(6)internet(1)}
```

ASN.1 基本上是一种原始的数据声明语言，除了上述 5 种基本数据类型以外，它还允许用户自定义原语对象，然后再把它们组合成复杂的构造对象。构造类型有 4 种方法，如表 7-2 所示。

表 7-2　构造类型说明

类型标识符	说　　明
SEQUENCE	一个或多个基本类型的有序集合
SEQUENCE OF	0 个或多个基本类型有序集合的数组
SET	一个或多个基本类型的无序集合
SET OF	0 个或多个基本类型无序集合的数组

2. ASN.1 转换语法

ASN.1 只能在设计时写在纸上，为了能够在实际的应用中也使用 ASN.1，设计者又定义了 ASN.1 的转换语法，它定义了 ASN.1 类型的值如何转换为适合于传输的字节序列。

ASN.1 转换语法是使用基本编码规则(Basic Encoding Rules，BER)进行二进制代码编写的。BER 的编写规则是：每一个传输的值，不论是固有的(原语)，还是用户自定义(构造)的，最多由 3 个字段组成：

- 标识符：包括类型和标记；
- 数据字段的长度，以字节为单位；
- 数据字段。

标识符位于第一个字段，它标识了后面的项，其本身有 3 个子字段，如表 7-3 所示。

表 7-3　标识符字段

Tag(6、7 位)	Type(5 位)	Number(4、3、2、1、0 位)

标识符最高两位编码(Tag)用来标识后面数据的作用，它共有 4 种选项，表 7-4 所示为其取值及含义。

表 7-4　标识符最高两位的取值及其含义

取值(二进制表示)	含　　义
00	表示通用的(Universal)
01	表示应用程序的(Application)
10	表示上下文相关的(Context specific)
11	表示私有的(Private)

标识符的下一位(Type)用来表示类型，取 0 时表示是原语类型(固有的)，取 1 时表示是构造类型(用户自定义的，由多个原语类型组成的“结构”体)。

标识符低 5 位(Number)用来标识后面数据的数据类型，类型及其标识代码如表 7-5 所示。类型也可自定，如果类型代码在 0～30 范围内时，直接使用即可，但当类型代码超过 30 时，Number(低 5 位)被置为 11111(二进制全 1)，然后在后面增加一到多个字节，这些字节的低 7 位用来表示数据，高 1 位表示是否结束，当高 1 位为 1 时表示是最后一个字节，其余的位均为 0。

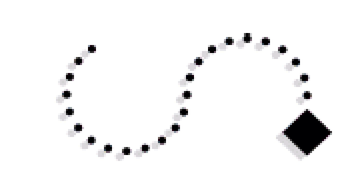


表 7-5　数据类型及其标识代码

数据类型标识符	代码	数据类型标识符	代码
INTEGER	2	OBJECT IDENTIFIER	6
BIT STRING	3	SEQUENCE and SEQUENCE OF	16
OCTET STRING	4	SET and SET OF	17
NULL	5		

例如，私有的复合结构，类型代码为 50 的 BER 编码的二进制形式是 11111111 10110010；通用的原语结构，标识为整型的 BER 编码的二进制形式是 00000010。

数据字段的长度位于标识符字段后，因为标识符字段是不定长的，所以数据字段的长度项具体位于第几字节，还要具体问题具体分析。

数据字段的长度项指出后面要用多少个字节来存储数据(注意：长度不包括这个字段本身和标识符字段)。

当数据长度小于 128 时，用 1 个字节来表示这个字段，其中最高位记为 0，其余低7 位用来表示长度；当长度的值大于 128 时，第 1 个字节用来表示用几个字节来表示长度，其中最高位记为 1，其余低 7 位用来表示长度值用了几个字节。

例如，要表示的数据长度为 15，则 BER 编码的二进制形式是 00001111；要表示的数据长度为 1000，则 BER 编码的二进制形式是 10000010 00000011 11101000，其中第一字节的最高位置 1，并且低 7 位的值是 2，表示后面有两个字节来表示数据长度，后两个字节表示实际的数据长度值 1000。

数据字段项是实际数据的存储位置，它的编码依赖当前数据的类型。

如果是 INTEGER 类型，则以二进制的补码方式编码，小于 128 的正整数需要用 1 个字节表示，小于 32 768 的正整数需要用 2 个字节表示，以此类推。

如果是 BIT STRING 类型，则编码内容不变，长度域表示需要用到的字节个数，并在实际的位串之前加一个字节表示位串最后一个字节不用的位数。比如，位串 010011111 被编码为 00000111 01001111 10000000，其中第一字节不是实际数据，它是表示最后一个字节有几个位不用，本例中的值是 7，也即表示最后一个字节中最高 1 位有效，其余均无效；第二个字节中存储的是位串前 8 位的值，第三个字节最高位中存放了位串的剩余 1 位，其余无效位均为 0。

如果是 OCTET STRING 类型，则编码内容不变。

如果是 NULL 类型，则长度域为 0，不传任何数据。

如果是 OBJECT IDENTIFIER 类型，则按 MIB 树的编码整数序列编码，每一项均按照整数编码，例如，因特网是{1,3,6,1}，但是，第一个数值总是 0、1 或 2，第二个数值总是小于 40，所以前两个数可用一个字节编码，因此因特网编码后的值是{43,6,1}。

BER 的编码规则非常复杂，如果没有实际的数据，就无法判断其会占有多少字节。下面列举一些例子加以说明。

INTEGER 类型的 50 的 BER 的二进制编码是 00000010 00000001 00110010，其中第一个字节是标识符，代表 INTEGER 型，第二个字节是长度，代表数值项占有一个字节。

BIT STRING 类型的“1110”的 BER 的二进制编码是 00000011 00000010 00000100



11100000，其中第一个字节是标识符，代表 BIT STRING 类型，第二个字节是长度，代表后面的数值占有两个字节，第三个字节表示位串的最后一个字节的后几位无效。

OCTET STRING 类型的“ab”的 BER 的二进制编码是 00000100 00000010 01100001 01100010，其中第一个字节是标识符，代表 OCTET STRING 类型，第二个字节是长度，代表实际数据占用两个字节，第三字节是“a”的 ASCII 码值，第四个字节是“b”的 ASCII 码值。

NULL 类型的 BER 的二进制编码是 0000101 00000000，其中第一个字节表示标识符，代表 NULL 类型，长度为 0，值域项没有。

OBJECT IDENTIFIER 类型的“{1.3.6.1}”的 BER 的二进制编码是 00000110 00000011 00101000 00000110 00000001，其中第一个字节表示标识符，代表 OBJECT IDENTIFIER 类型，长度为 3，代表实际数据共占有三个字节（“{1.3}”两个值共占一个字节），第三个字节表示“{1.3}”，第四个字节表示“{6}”，第五个字节表示“1”。

3. SMI

在实际的设备中所有的管理信息和对象都存放在库中(MIB)，为了方便人们的记忆和管理，设计者使用了一个有层次的树型结构来表示这些管理对象。SMI 对于 MIB 来说就相当于模式对于数据库。SMI 定义了每一个对象“看上去像什么”。图 7-2 所示为 SMI 定义的 MIB 树的顶部。

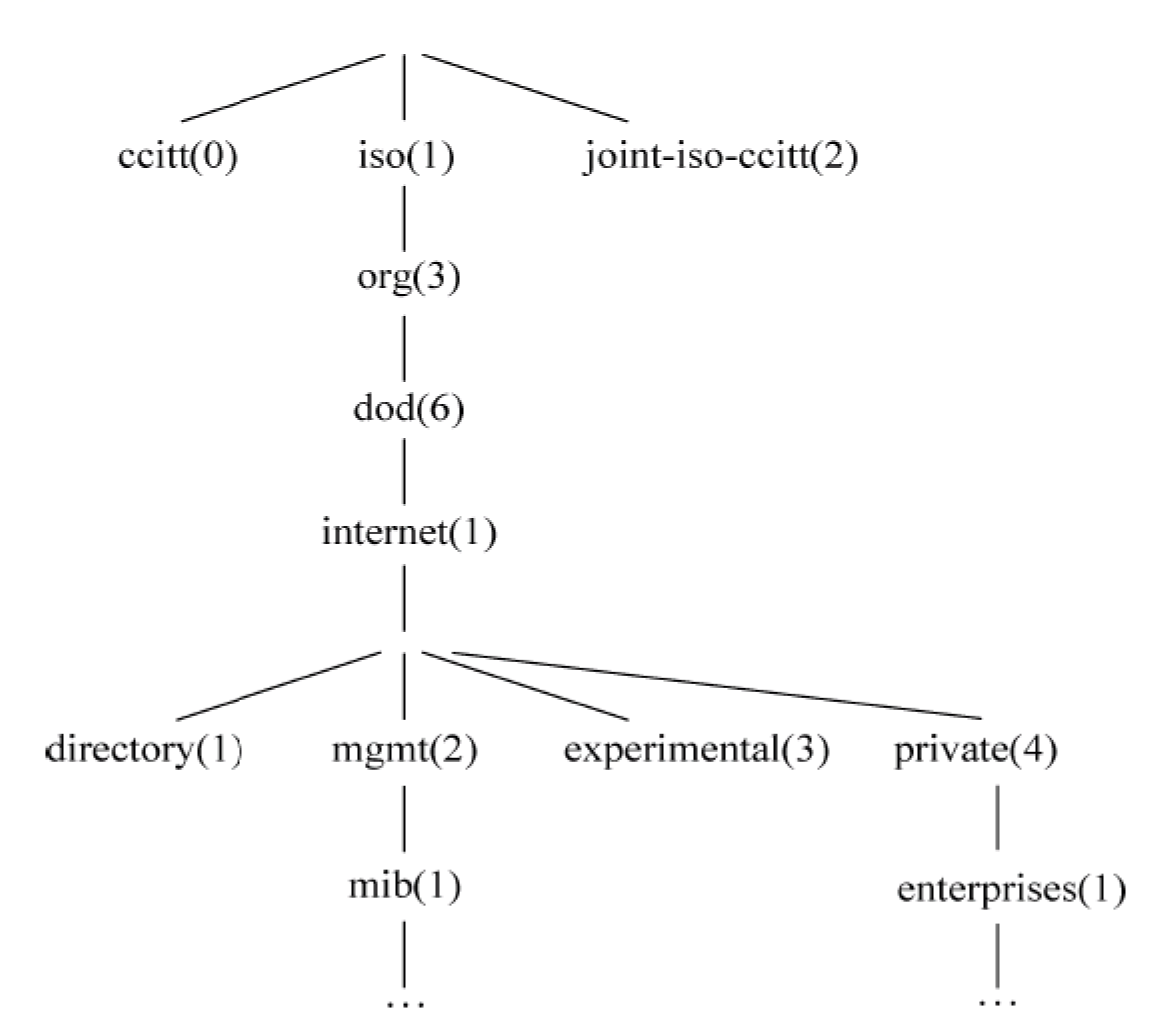
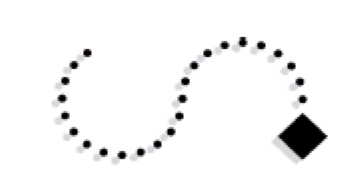


图 7-2　RFC 1155(SMI)定义的 MIB 树的顶部

在这个树型结构中，internet 对象可以由以下代码标识：{iso(1) org(3) dod(6) internet(1)}或者简记为{1.3.6.1}。

这种标识方法叫做对象标识符(Object Identifier，OID)，用于标识一个管理对象，以及在 MIB 中如何访问该对象。每一个 OID 在整个 MIB 树中都是惟一的，就如同实际生活中每一个中华人民共和国的公民都会有一个与自己相对应的身份证号，这个号码由省(或直辖市等)号、市号、出生年月、编号以及校验码组成，这种按层次的组成方法可以保证每一个人都有一个惟一的号码，而且通过这种方法可以非常容易地记忆和查询。



SMI 不定义 MIB 对象，但其规定了定义管理对象的格式。一个对象定义通常包括 5 个域。

① OBJECT：是一个字符串名，它叫 OBJECT DESCRIPTOR，它指定对象类型，这个类型和 OBJECT IDENTIFIER 相对应。

② SYNTAX：对象类型的抽象语法。它必须可以解析到 ASN.1 类型 ObjectSyntax 的一个实例上。

③ DEFINITION：对象类型语义的文本描述。实现中必须保证对象的实例满足这个定义，因为这个 MIB 是用于多厂商环境中的，要照顾到它们的情况。对象在不同的机器上有相同的意义是很重要的，这要靠文本约束。

④ ACCESS：取只读、读写、只写或不能访问这 4 个值。

⑤ STATUS：强制（mandatory）、可选（optional）或过时的（obsolete）。

其中，语法是根据对象类型定义对象结构，定义时使用 ASN.1，但 ASN.1 中的一些通用化需要加以限制。SMI 中使用 3 种语法：原始类型、构造类型和自定义类型。

原始类型和构造类型在 7.1 节中已经讲解过了。原始类型包括 INTEGER、OCTET STRING、OBJECT IDENTIFIER 和 NULL 等。构造类型使用 SEQUENCE 或 SEQUENCE OF 建立行或表。

SMI 允许在一个新应用产品的范围内由用户自定义类型，但这些类型必须能够分解为基本类型、行、表或其他自定义类型。SMI 中定义了用于 SNMP 的一些自定义类型，其类型值和说明如表 7-6 所示。

表 7-6　SMI 自定义类型值及其说明

SMI 自定义类型值	说　明
NetworkAddress	此类型代表多个可能的协议族中的一个地址格式，当前只有 Internet 协议族
IpAddress	此类型代表 32 位的 IP 地址，表示为长度为 4 的字符串。在 ASN.1 类型使用 BER 规则进行编码时，只能使用原始编码形式
Counter	此类型代表一个非负整数，它只能增加，直到最大值。当达到最大值后，它会返回 0 重新开始。RFC 1155 指定此类型的最大值为 2^32－1，也就是 4 294 967 295。此类型也称为循环计数器，是定义对象时常见的类型之一。此类型的典型应用是对接收或发送的数据包和字节的数目计数
Gauge	此类型代表一个非负整数，它可以增加或减少，但在最大值时停止。RFC 1155 指定此类型的最大值为 2^32－1，也就是 4 294 967 295
TimeTicks	此类型为非负整数，用于记录从一时间点起经过了多少个百分之一秒的时间。此类型是和计时器相关的，是两个时间点的差值，所以定义时需要在描述里告诉用户这两个时间参考点
Opaque	此类型支持对 ASN.1 语法进行扩充。此类型只要求接收方能够对数据进行解密，并没有要求接收方一定要理解其内容
DisplayString	可打印的字符串，使用可读的字符，是一种方便阅读的类型。定义为：DisplayString∷＝OCTET STRING
PhysAddress	存放接口的 MAC 地址。定义为：PhysAddress∷＝OCTET STRING

图 7-3 所示为两个 SMI 的例子。第一个例子是叫做 lostPackets 的变量，它用于路由器或其他处理分组的设备。第二个例子是叫做 ipAddrTable 的变量，它用于描述地址表，其类型是一个构造类型，::=符号后的值指明它在 MIB 树上的位置。

```
lostPackets OBJECT-TYPE
    SYNTAX Counter              --use a 32-bit counter
    ACCESS read-only            --the management station may not change it
    STATUS current              --this variable is not obsolete (yet)
    DESCRIPTION
        "The number of packets lost since the last boot."
    ::= {experimental 20}


ipAddrTable OBJECT-TYPE
    SYNTAX
        ipAddrEntry ::= SEQUENCE{
                ipAdEntAddr
                    ipAddress,
                ipAdEntIfIndex
                    INTEGER,
                ipAdEntNetMask
                    ipAddress,
                ipAdEntBcastAddr
                    INTEGER,
                ipAdEntReasmMaxSize
                    INTEGER (0..65535)
                }
    ACCESS not-accessible
    STATUS mandatory
    DESCRIPTION
        "The table of addressing kinformation relevant to this entity's IP address."
    ::= {ip 20}
```

图 7-3 SMI 定义示例

7.2.2 MIB-2 功能组

在 RFC 1156 文档中定义了 SNMP 的第一个版本的管理信息库(MIB-1)，随后又在 RFC 1213 文档中定义了第二个版本的管理信息库(MIB-2)。MIB-2 是对 MIB-1 进行的扩展和修改，现在的 SNMP 都是以 MIB-2 为基准。

1. MIB-2 功能组的组成

MIB-2 功能组由 9 个功能组组成。

① system 组：提供运行代理的设备或系统的全部信息。

② interfaces 组：包含关于系统中网络接口的信息。

③ at 组：用于 IP 地址到数据链路地址的地址转换表，但是这个组随着 RFC 1213 的引退而逐渐被放弃了，其内容也被移到了其他的文档(组)中。

④ ip 组：包含关于设备的 IP 地址的信息。

⑤ icmp 组：包含关于设备的 Internet 控制消息协议的信息。

⑥ tcp 组：包含关于设备的传输控制协议的信息。

⑦ udp 组：包含关于设备的用户数据报协议的信息。

⑧ egp 组：包含关于设备的外部网关协议的信息，随着 SNMP 的发展，这个组现在也已经不再使用了。

⑨ snmp 组：包含关于设备的简单网络管理协议的信息。

图 7-4 所示为 MIB-2 的组成图。

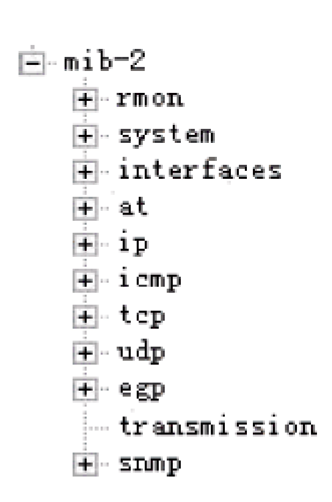


图 7-4　MIB-2 组成图

2. MIB-2 功能组常用的对象

下面简单介绍一些常用的对象，详细的介绍读者可以参考相关资料。

① sysDescr 对象，用于设备或实体的描述。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. system. sysDescr(或记为. 1. 3. 6. 1. 2. 1. 1. 1)。

② sysObjectID 对象，用于描述设备厂商的授权标识符。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. system. sysObjectID(或记为. 1. 3. 6. 1. 2. 1. 1. 2)。

③ sysName 对象，用于描述设备的名字，可能是官方的主机名或者是分配的管理名字。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. system. sysName(或记为. 1. 3. 6. 1. 2. 1. 1. 5)。

④ ifNumber 对象，用于描述本地系统中包含的网络接口总数。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifNumber(或记为. 1. 3. 6. 1. 2. 1. 2. 1)。

⑤ ifDescr 对象，用于描述接口的一个字符串描述，包括从操作系统获得的接口名，可能包括 eth0、ppp0 和 lo0 等值。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifDescr (或记为. 1. 3. 6. 1. 2. 1. 2. 2. 1. 2)。

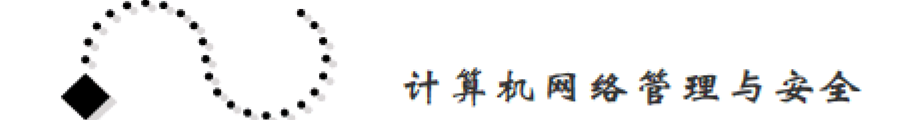
⑥ ifType 对象，用于描述接口的类型。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifType(或记为. 1. 3. 6. 1. 2. 1. 2. 2. 1. 3)。

⑦ ifMtu 对象，用于描述接口的最大传输单元，即接口上可以发送或接受的最大帧。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifMtu(或记为. 1. 3. 6. 1. 2. 1. 2. 2. 1. 4)。

⑧ ifSpeed 对象，用于描述接口速率(容量)。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifSpeed(或记为. 1. 3. 6. 1. 2. 1. 2. 2. 1. 5)。

⑨ ifPhysAddress 对象，用于描述接口的数据链路地址(物理地址)。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifPhysAddress(或记为. 1. 3. 6. 1. 2. 1. 2. 2. 1. 6)。

⑩ ifAdminStatus 对象，用于描述接口的管理状态，该状态是 ifOperStatus 对象中列出的已定义状态之一。其 OID 是：. iso. org. dod. internet. mgmt. mib-2. interfaces. ifAdminStatus(或记为. 1. 3. 6. 1. 2. 1. 2. 2. 1. 7)。



⑪ ifOperStatus 对象，用于描述接口当前的操作状态，其状态包括 up (1)、down (2) 和 testing (3)。其 OID 是：.iso.org.dod.internet.mgmt.mib-2.interfaces.ifOperStatus (或记为.1.3.6.1.2.1.2.2.1.8)。

7.3 SNMP 通信模型

简单网络管理协议(SNMP)最初是由因特网工程任务组织(IETF)的研究小组为了解决因特网上的路由器管理问题而提出的。SNMP 被设计成与协议无关，可以在 IP、IPX、AppleTalk、OSI 以及其他用到的传输协议上使用。SNMP 包括一系列协议组和规范，提供了一种从网络上的设备中收集网络管理信息的方法，同时也为设备向网络管理站报告问题。

SNMP 的结构分为 SNMP 管理者和 SNMP 代理两部分。管理者从代理中收集数据有两种方法：一种是只轮询的方法，另一种是基于中断的方法。

只轮询的方法，是由管理者每间隔一段时间，向各个代理依次发送询问信息，然后由代理返回查询结果，这种方法可以使代理总是在管理者的控制之下。只轮询方法的缺陷在于信息的实时性比较差。因为如果轮询间隔太小，那么将产生太多不必要的通信量。如果轮询间隔太大，并且在轮询时顺序不对，那么对于一些大的灾难性的事件的通知就会太慢。

基于中断的方法是当有异常事件发生时，由代理主动向管理者发送信息，使管理者可以及时地了解网络设备的状态。基于中断的方法也有一定的缺陷，当异常事件发生且要传送的信息量较大时，这种方法需要消耗大量的系统资源，从而影响了代理执行主要的功能，另外当多个代理同时发生中断时，网络将变得非常拥挤。

SNMP 结合上述两种方法的优点和缺点，形成了面向自陷的轮询方法，它是执行网络管理最为有效的方法。一般情况下，管理者通过轮询代理进行信息收集，在控制台上用数字或图形来显示这些信息，提供对网络设备工作状态和网络通信量的分析和管理功能。当代理设备出现异常状态时，代理通过 SNMP 自陷立即向网络管理者发送通知。SNMP 定义了 get、get-next 和 set 3 种基于轮询的操作，并且还定义了基于中断的 trap 操作。

7.3.1 SNMP 协议数据单元

SNMP 的工作原理非常简单，在管理者和代理之间实时传递信息，这些信息被称为协议数据单元(PDU)，在 SNMP 中一共定义了 4 类协议数据单元，如图 7-5 所示为这 4 种操作的示意图。

SNMP 协议被封装在 UDP 协议中，前 3 种操作使用 UDP 的 161 端口，由代理发出的 trap 操作使用 UDP 的 162 端口。图 7-6 所示为 SNMP 4 种操作的报文格式。

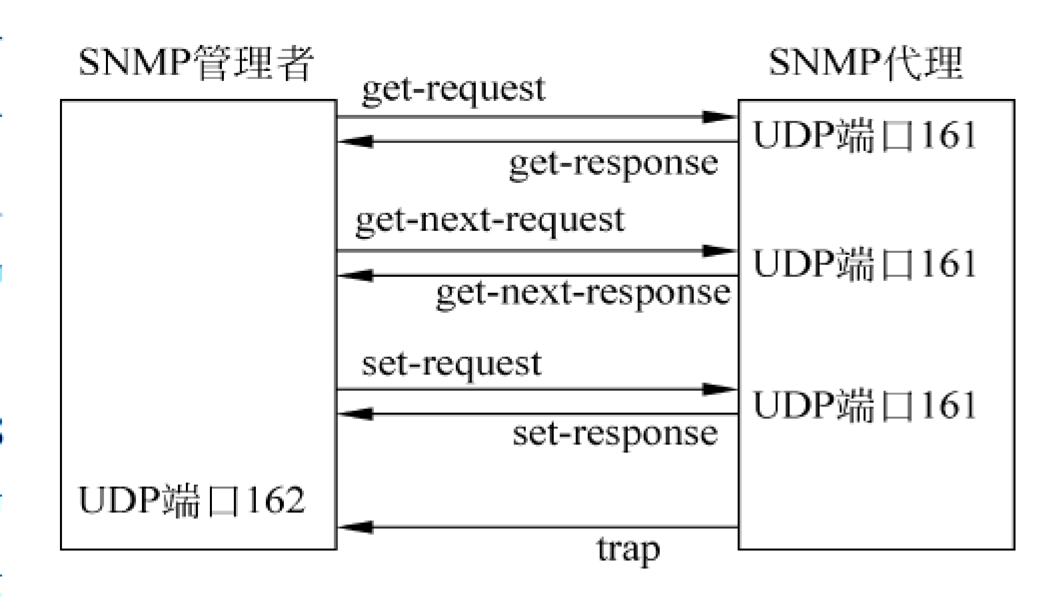


图 7-5　SNMP 4 种报文的操作示意图

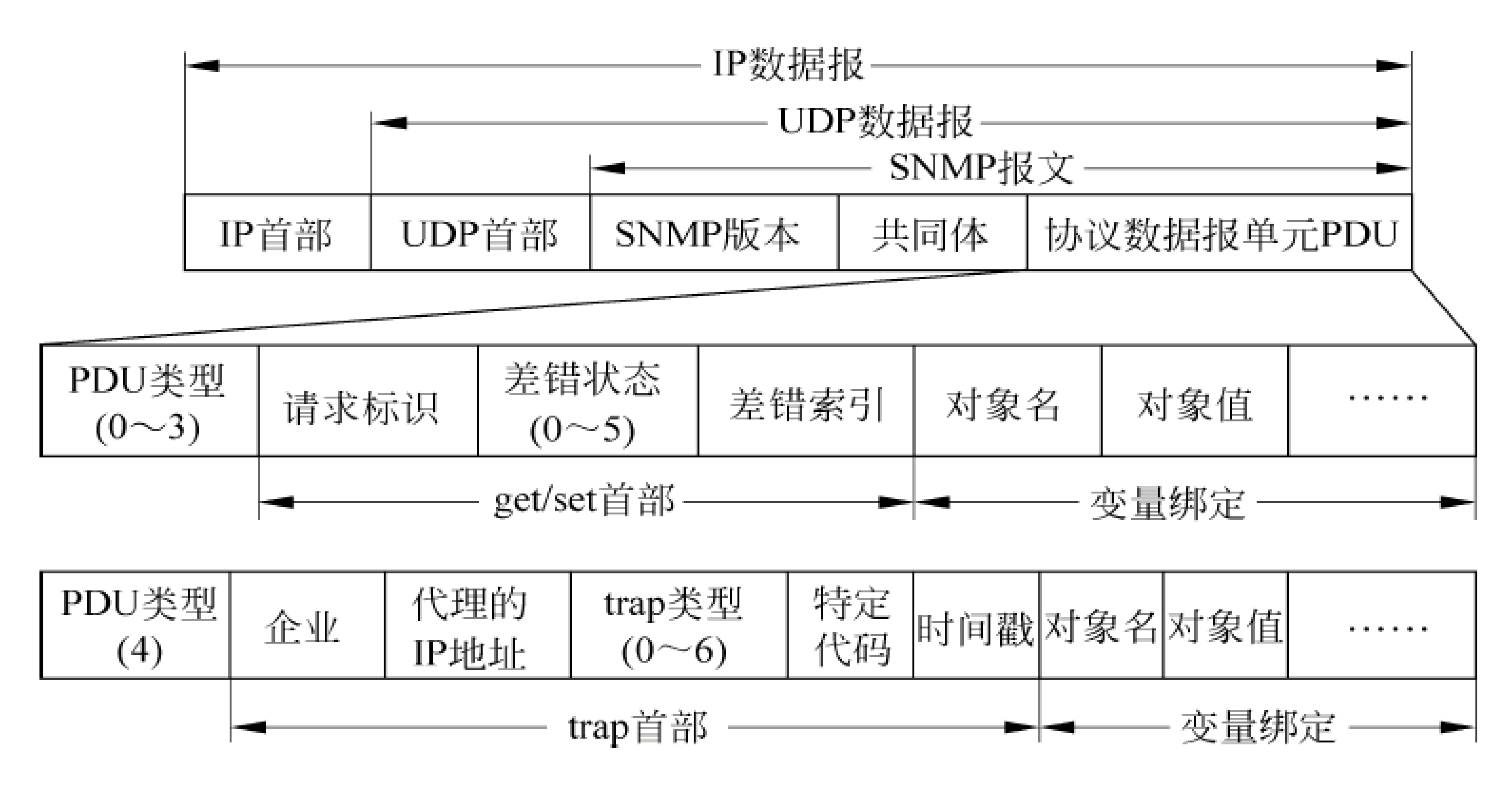


图 7-6　SNMP 报文格式

1. SNMP 版本与共同体

SNMP 的报文一般包括 3 个部分：SNMP 版本、共同体和协议数据单元(PDU)。

SNMP 版本用于标识管理者和代理使用的是哪个版本的 SNMP 协议，到现在为止可以使用的 SNMP 版本共有 3 个，分别是：SNMPv1、SNMPv2 和 SNMPv3。在 SNMP 版本中存放的版本值比实际应用的版本号小 1。例如，管理者或代理使用的是 SNMPv1，则这项的值是 0。

共同体是一个字符串，作为管理者与代理之间的明文口令，常用的是 6 个字符，值是"public"，该值可以由管理员设置。

协议数据单元(PDU)是 SNMP 报文的主要内容所在，它有两种报文类型：get/set 报文和 trap 报文。

2. get/set 报文

get/set 报文是基于轮询的操作，是由管理者首先向代理发出查询或设置命令，然后由代理返回操作结果。get/set 报文主要包括 PDU 类型、请求标识、差错状态、差错索引和变量绑定 5 部分。

PDU 类型用来表示 SNMP 报文的功能，共有 5 个值可以使用，如表 7-7 所示。PDU 类型项中的值是一个特殊类型(上下文相关的构造类型)的值，只用一个字节来表示。

表 7-7　PDU 类型

PDU 类型	名　称	二进制值	十六进制值
0	get-request	10100000	0xa0
1	get-next-request	10100001	0xa1
2	get-response	10100010	0xa2
3	set-request	10100011	0xa3
4	trap	10100100	0xa4

请求标识是由管理进程设置的一个整数值。每一个进程都有一个相应的标识，使管理进程能够识别返回的响应报文对应于哪一个请求报文，同一对请求报文和响应报文使用同一个标识。

差错状态是由代理设置的一个值，用于标识返回的报文是否有错，以及出现了什么样的错误。差错状态有 6 个值可以使用，如表 7-8 所示。

表 7-8　差错状态

差错状态	名　　称	描　　述
0	noError	没有错误
1	tooBig	代理进程无法把响应放在一个 SNMP 消息中发送
2	noSuchName	操作一个不存在的变量
3	badValue	set 操作的值或语义有错误
4	readOnly	管理进程试图修改一个只读变量
5	genError	其他错误

差错索引也是一个由代理设置的值，用来指明差错发生哪个变量上（即变量列表中的偏移）。注意，并不是所有差错都有差错索引，只有发生差错 2、3 和 4 时才会有差错索引。

变量绑定是由一个或多个对象名和对象值对组成。如果是 get-request 和 get-next-request 操作，对象名由管理者设置，并把对象值设置为空（NULL）类型，代理收到后就根据对象名查询对应的对象值，如果找到，则把对象名和对象值返回给管理者。如果是 set-request 操作，则对象名和对象值均由管理者设置，代理收到后只把对应的对象名的值改为管理者设置的对象值。变量绑定中可以出现多个对象名和对象值对，即一个 SNMP 报文可以查询（get 操作）或设置（set 操作）多个对象。

3. trap 报文

trap 报文是基于中断的操作，当代理设备发生异常时，代理即向管理者发送这个报文。trap 报文主要包括 PDU 类型、企业、代理的 IP 地址、trap 类型、特定代码、时间戳和变量绑定 7 部分。

PDU 类型在 trap 报文中固定为 4。

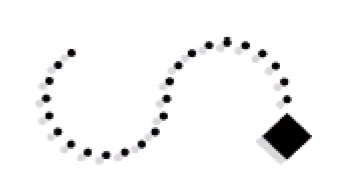
企业项是 trap 报文的网络设备的对象标识符。此对象标识符在 MIB 树上的 enterprises 节点{1.3.6.1.4.1}（见图 7-2）下面的一棵子树上。

代理的 IP 地址项标明代理设备的 IP 地址是何值。

trap 类型标明 trap 报文的类型，共有 7 种选项，如表 7-9 所示。

表 7-9　trap 类型

trap 类型	名　　称	说　　明
0	coldStart	代理进行了初始化
1	warmStart	代理进行了重新初始化
2	linkDown	一个接口从工作状态变为故障状态
3	linkUp	一个接口从故障状态变为工作状态
4	authenticationFailure	从 SNMP 管理进程接收到一个具有无效共同体的报文
5	egpNeighborLoss	一个 EGP 相邻路由器变为故障状态
6	enterprisespecific	在这个特定的代码字段中查找 trap 信息



trap 类型为 2、3、5 时，在报文后面变量部分的第一个变量对应标识响应的接口。

时间戳项指明自代理进程初始化到 trap 报告的事件发生所经历的时间，单位为 10ms。

变量绑定的内容与 get/set 报文中的变量绑定相同。

7.3.2 SNMP 的安全机制

在网络管理系统的代理设备上存放着大量的管理信息库，它们的安全直接影响到整个网络系统的安全。为了保证代理能够保护其自身以及 MIB，使 MIB 能够拒绝非法的访问，代理需要设置一些安全机制。

在 SNMP 中，代理不但要控制自己本地的 MIB，而且必须控制多个管理者对该 MIB 的使用。这种控制包含 3 个方面。

- 认证服务。代理可以把对 MIB 的访问权限限制为已被授权的管理者。
- 访问策略。代理可以给不同的管理者不同的访问特权。
- 转换代理服务。一个代理可以作为其他被管理站的转换代理，包括在转换代理系统中，为其他的被管理系统实现认证服务或访问策略。

1. SNMPv1 的安全机制

SNMPv1 是 SNMP 的第一个版本，其安全性上的设计非常简单，仅仅提供了有限的安全机制，即共同体的概念。

共同体的概念在 7.3.1 小节中已经提到过，它是一个明文的字符串，每一个 SNMP 共同体都是一个在 SNMP 代理和多个 SNMP 管理者之间定义的认证、访问控制和转换代理的关系。管理者发送的每一个报文中，都必须填写好对应的共同体项，代理收到这些报文后比对共同体的内容，如果正确则被允许访问对应的对象，反之则被拒绝。共同体在这里起到密码的作用，如果发送者知道这个密码，就认为该信息通过了认证，是可靠的。

共同体不但有认证的功能，还有设置访问权限的功能。一条已通过认证的信息对 MIB 有何访问权限也是通过共同体来实现的。代理为每一个共同体定义了一个 SNMPv1 共同体框架文件，该框架文件包括两部分。

- MIB 视图。MIB 中对象一个子集，对不同的共同体可以定义不同的视图，属于同一视图的对象不必同属于一个 MIB 子树。
- 访问模式。共同体可以定义一种访问模式。

2. SNMPv2 的安全机制

由于 SNMPv1 的安全机制过于简单，因此 SNMPv2 加强了安全的考虑。SNMPv2 具有支持分布式网络管理、扩展数据类型、可以实现大量数据的同时传输、丰富故障处理能力、增加集合处理功能、加强数据定义语言等特点。

此外，SNMPv2 还引入了上下文的概念。上下文是一个可被 SNMPv2 实体访问的被管理对象资源的集合，分为本地上下文和远程上下文，本地上下文被标识为一个 MIB 视图，远程上下文被标识为一个转换代理关系。

使用了上下文的访问控制策略由以下 4 个元素组成。

- 目标：SNMP 参加者按主体方的请求执行管理操作。
- 主体：SNMP 参加者请求目标方执行管理操作。

- 资源：管理操作在其上执行的管理信息，可表示为一个本地 MIB 视图或一个代理关系，资源也被称为上下文。
- 权限：对于一个特定的上下文可允许的操作，这些操作可用允许的协议数据单元定义，由目标代表主体执行。

但是，SNMPv2 并没有完全实现预期的目标，尤其是安全性能没有得到提高，如身份验证、加密、授权和访问控制、适当的远程安全配置和管理能力等都没有实现。1996 年发布的 SNMPv2C 是 SNMPv2 的修改版本，然而就在新的文件刚刚发布时就有人发现其安全方面存在重要缺陷，而且改进安全设施的工作又迟迟没有进展，最后决定丢掉安全功能，把增加的其他功能作为新标准颁布，并保留了 SNMPv1 的报文封装格式，继续使用 SNMPv1 的基于明文密钥的身份验证方式。

3. SNMPv3 的安全机制

1998 年 1 月 IETF 提出了互联网建议 RFC 2271～RFC 2275，正式形成了 SNMPv3。这一系列文件定义了包含 SNMPv1 和 SNMPv2 所有功能在内的体系框架以及包含验证服务和加密服务在内的全新的安全机制，同时还规定了一套专门的网络安全和访问控制规则。RFC 2271 定义的 SNMPv3 体系结构体现了模块化的设计思想，可以简单地实现功能的增加和修改。其特点主要有：

① 安全性好：具有多种安全处理模块。

② 适应性强：适用于多种操作环境，既可以管理最简单的网络，实现基本的管理功能，又能够提供强大的网络管理功能，满足复杂网络的管理需求。

③ 扩充性好：可以根据需要增加模块。

SNMPv3 主要有 3 个模块：信息处理和控制模块、本地处理模块和用户安全模块。

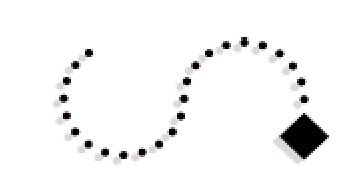
（1）信息处理和控制模块在 RFC 2272 中定义，负责信息的产生和分析，并判断信息在传输过程中是否要经过代理服务器。

（2）本地处理模块的主要功能是进行访问控制，处理打包的数据和中断。访问控制是指通过设置代理的有关信息使不同管理者的管理进程在访问代理时具有不同的权限，在协议数据单元一级完成。访问控制的策略必须预先设定。SNMPv3 通过使用带有不同参数的原语来灵活确定访问控制方式。

（3）用户安全模块。与前两个版本相比，SNMPv3 增加了 3 个新的安全机制：身份验证，加密和访问控制。其中，访问控制功能由本地处理模块完成，而身份验证和数据保密服务则由用户安全模块提供。身份验证是指代理或管理者接到信息时必须确认信息是否来自授权的管理者或代理，以及信息在传输过程中是否改变。这个功能的实现要求管理者和代理必须共享同一密钥。管理者使用密钥计算验证码，然后将其加入信息中，而代理则使用同一密钥从接收的信息中提取出验证码，从而得到信息。加密的过程与身份验证类似，也需要管理者和代理共享同一密钥来实现信息的加密和解密。SNMPv3 使用私钥和验证密钥来实现身份验证和加密功能。

7.3.3 SNMP 的操作

SNMP 共有 4 种操作，分别是 get-request、get-next-request、set-request 和 trap，这些



操作可以完成查询或设置简单对象、查询未知对象、查询或设置表对象和陷入操作等功能。

1. 查询或设置简单对象

查询简单的对象值可以用 get-request 操作，代理响应的是 get-response 报文。如果变量绑定项中含有多个对象名，则一次可以查询多个对象的值。接收 get-request 的 SNMP 实体以请求标识相同的 get-request 响应。特别要注意的是 get-request 操作的原子性，即如果所有请求的对象值都可以得到，则给予应答；反之，只要有一个对象的值得不到，则可能返回下列错误条件之一：

① 变量绑定项中的一个对象无法与 MIB 中的任何对象名匹配，或者要检索的对象是一个复杂类型(比如子树或表等)，其没有对象实例生成，那么在这些情况下，代理返回的 PDU(即 get-response)中差错状态字段置为 noSuchName，错误索引字段设置为出错的对象名在变量绑定中的偏移量，变量绑定项中不返回任何值。

② 代理设备中的响应实体可以提供所有要检索的值，但是所请求的变量太多，一个响应 PDU 装不下，这往往是由下层协议数据单元大小限制的。这时响应实体返回一个应答 PDU，其差错状态字段置为 tooBig。

③ 由于其他原因(例如代理不支持等)，代理中的响应实体至少不能提供一个对象的值，则返回的 PDU 中差错状态字段置为 genError，错误索引字段设置为出错的对象名在变量绑定中的偏移量，变量绑定项中不返回任何值。

设置简单的对象值可以用 set-request 操作，代理用于响应的同样也是 get-response 报文。set-request 操作也可以一次含有多个对象名，如果所有的对象都可以修改，则修改所有请求的对象的值；如果至少有一个对象不能修改，则所有请求的对象的值均不被修改，并在差错状态字段中指明出错原因(例如对象是只读的)。

2. 查询未知对象

如果不能确定对象的名称，则可以用 get-next-request 操作查询指定对象名的下一个对象实例，但是并不要求指定的对象名或者是子树的对象标签必须存在。get-next-request 还可以遍历整个 MIB 树。

3. 查询或设置表对象

set-request 操作用于修改对象的值，它的操作与对简单对象操作类似。get-next-request 操作可以查询表对象，或是遍历整个 MIB 树。

4. 陷入操作

陷入操作是由代理向管理者发出的异步事件警告，它不需要应答报文。SNMP 规定了 6 种陷入条件：

① coldStart 发送实体重新初始化，代理的配置已经改变。这种情况经常是由系统失效引起的。

② warmStart 发送实体重新初始化，但代理的配置没有改变。这种情况是正常的重启动过程。

③ linkDown 链路失效通知，其中变量绑定项的第一项指明对应接口表的索引对象及其值。

④ linkUp 链路启动通知，其中变量绑定项的第一项指明对应接口表的索引对象及其值。

⑤ authenticationFailure 发送实体收到一个没有通过认证的报文。

⑥ egpNeighborLoss 相邻的外部路由器失效或关机。

⑦ enterpriseSpecific 由设备制造商定义的陷入条件，在特殊陷入字段项中指明具体的陷入类型。

7.3.4 SNMP 通信示例

前面介绍了 SNMP 的操作功能以及 MIB-2 功能组的组成，下面通过实例来看一看 SNMP 报文的组成以及它是如何传输的。

1. Microsoft 网络监视器

网络的底层就是数据包，只有了解这些在网络上传输的数据包，才能真正认识网络系统。现在有很多网络数据包的捕获工具，例如，SnifferPro、Ethereal 等。这些工具功能强大、操作方便、界面友好，是网络管理员维护网络必不可少的工具。

虽然这些工具非常好用，但是有些工具需要花钱购买，有些工具则安装非常复杂，因此本书并没有采用这些工具，而是使用了微软公司在 Windows Server 2000（或以上）和 Windows Server 2003 版本上自带的 Microsoft 网络监视器。

选择"开始"→"程序"→"管理工具"→"网络监视器"命令，打开 Microsoft 网络监视器，如图 7-7 所示。

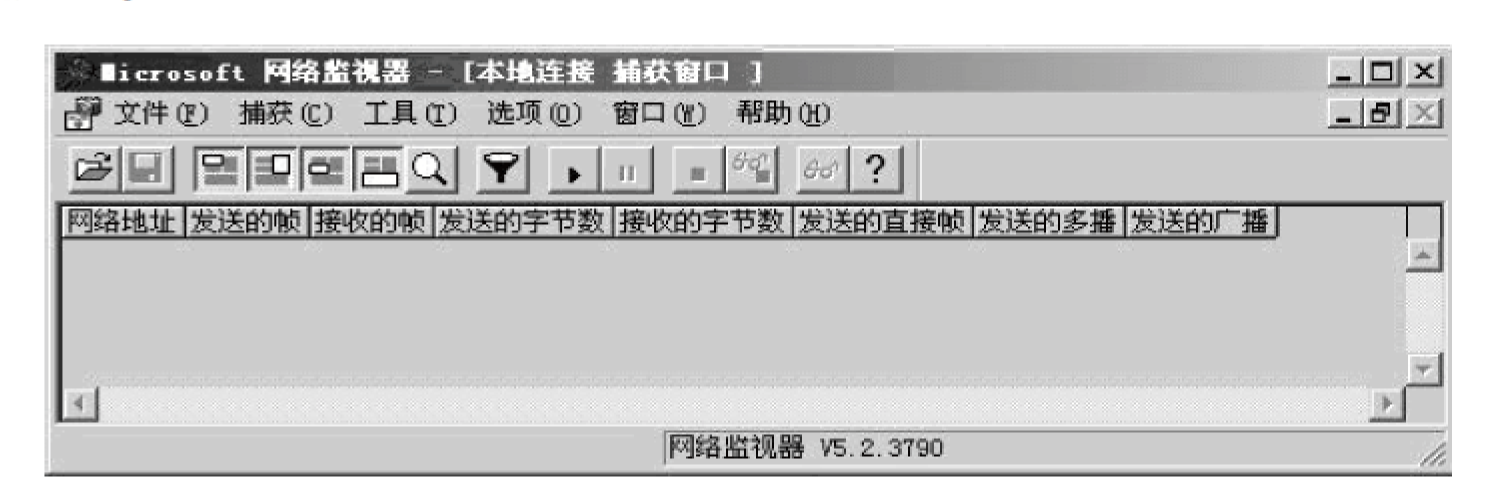
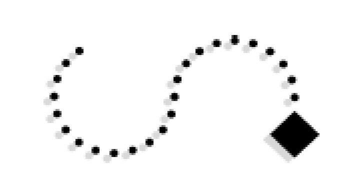


图 7-7 "Microsoft 网络监视器"窗口

如果是第一次使用，则在刚打开 Microsoft 网络监视器时会弹出如图 7-8 所示的"选择一个网络"对话框，在该对话框中用户可以选择想要监视的网络接口，这里选择"本地连接"，单击"确定"按钮。如果在使用过程中需要改变被监视的网络接口，则可以在"Microsoft 网络监视器"窗口中选择"捕获"→"网络"命令，也可以打开这个对话框。



图 7-8 "选择一个网络"对话框



选择好网络接口后就可以开始监视了，单击图 7-7 工具栏中的“开始”按钮，监视器就会监听从这时起的所有网络数据包。如果需要查看数据包的详细内容，则可以单击“停止并查看”按钮，弹出如图 7-9 所示的捕获窗口。如果用户对某一个数据包感兴趣，可以双击这个数据包，以便更详细地了解该数据包的内容。



图 7-9 捕获窗口

Microsoft 网络监视器还有很多其他功能，由于篇幅有限，这里就不一一介绍了，读者如果有兴趣，可以参看相关的参考资料。

2. Getif

Getif 是一款免费使用的简单网络管理工具，是通过 SNMP 协议访问被管理的设备，其主界面如图 7-10 所示。

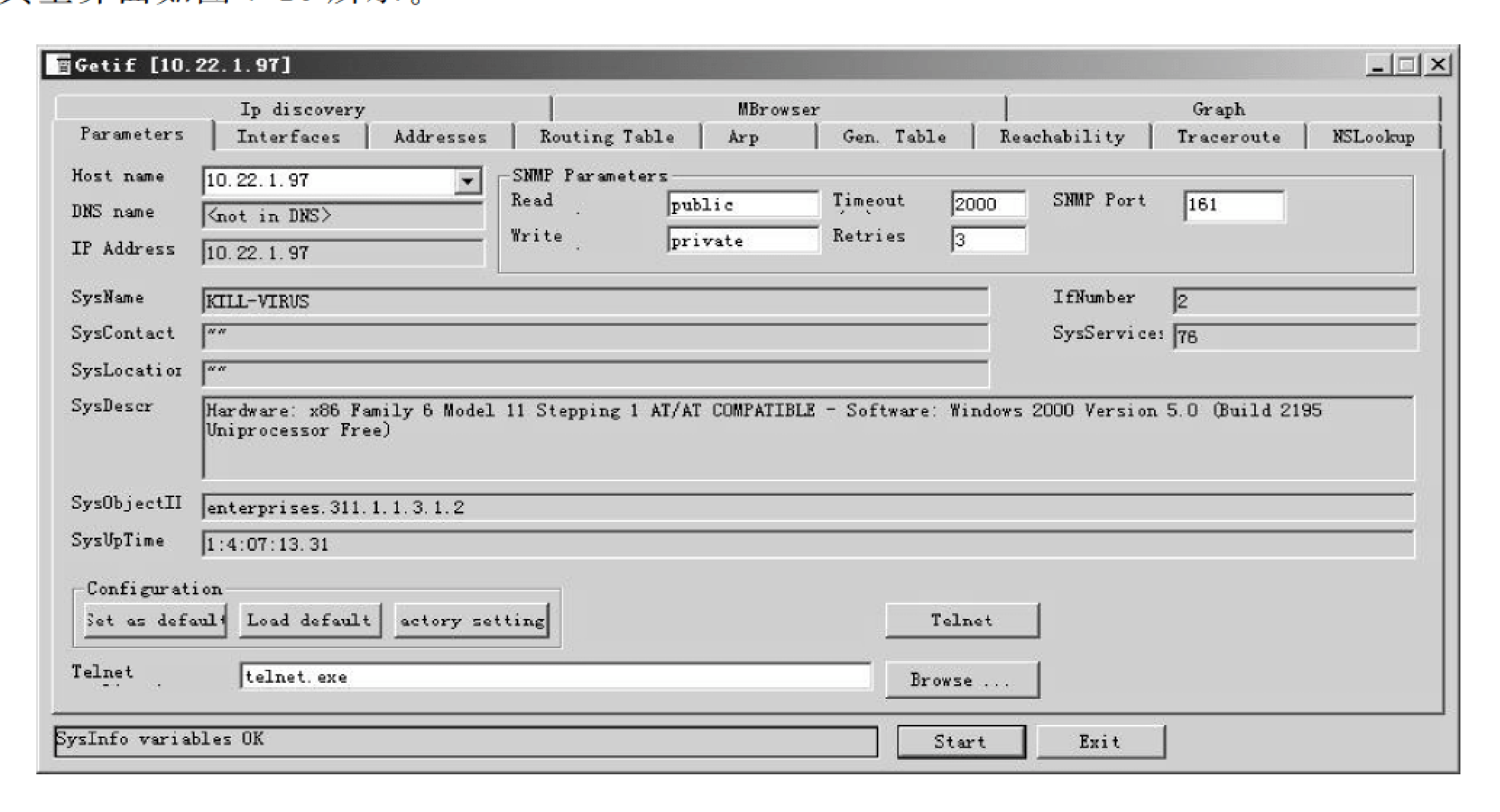


图 7-10 Getif 主界面

首先在 Host name 组合框中输入要访问的设备的 IP 地址，然后在 SNMP Parameters 选项组中的 Read 和 Write 文本框中输入共同体的值（默认是 public 和 private），最后单击 Start 按钮即可。如果被管理设备可以正常访问，则会返回相应的参数，如果被管理设备不能正

常访问，则在窗口最下面的状态栏中显示相应的错误信息。

Getif 工具有很多功能，包括网络接口查看(Interface)、地址查看(Address)、路由表查看(Routing Table)、ARP 地址查看(Arp)、IP 地址发现(IP discovery)等。由于篇幅有限，这里就不一一介绍了，读者如果有兴趣，可以参看相关的参考资料。这里主要介绍 MBrowser 功能，该功能是以树型的方式查看 MIB。MBrowser 选项卡如图 7-11 所示。

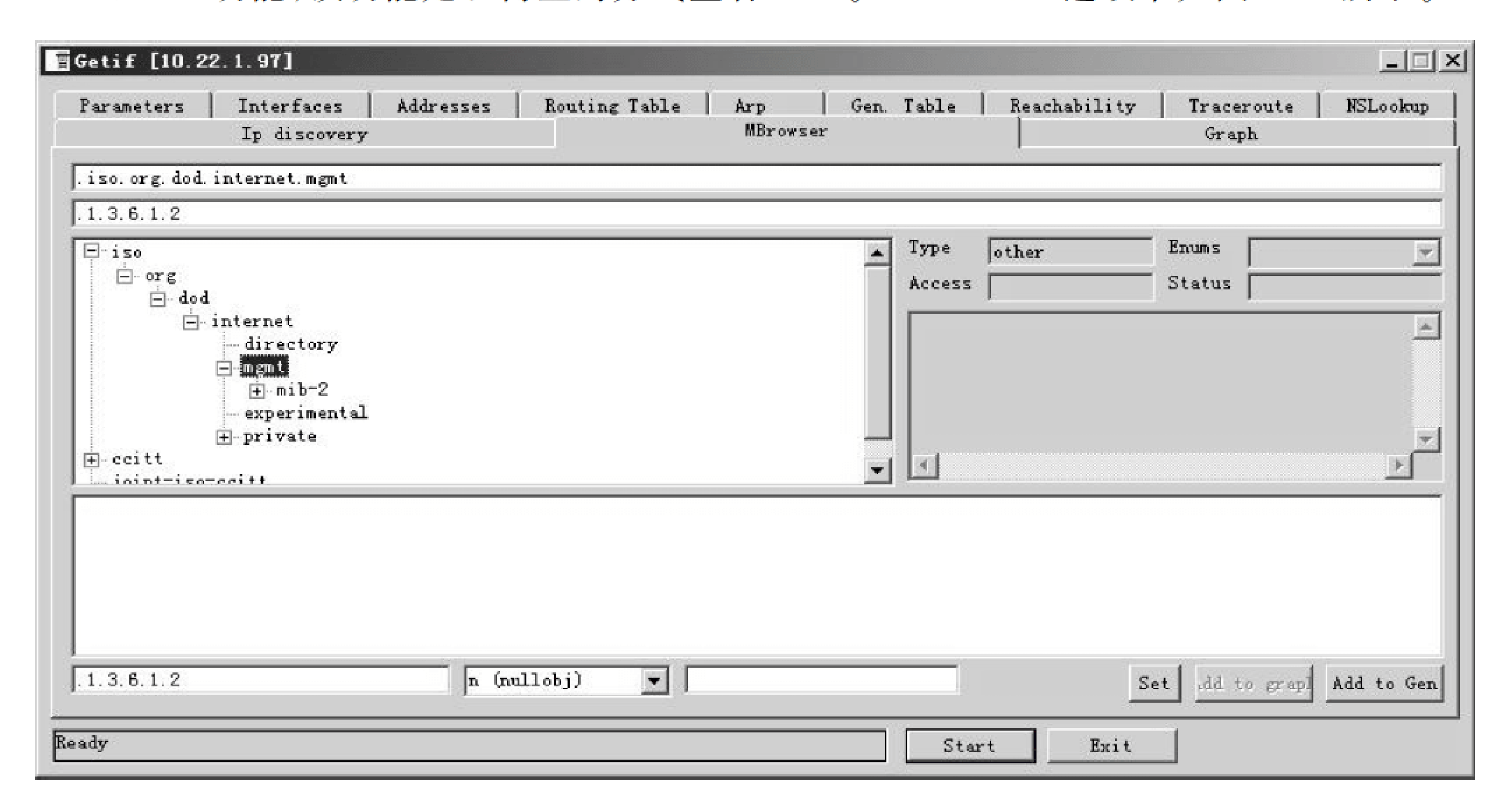


图 7-11　MBrowser 选项卡

第一个文本框中显示 OID 标识，第二个文本框中显示数字 OID 标识，中间的左侧部分显示树型结构，右侧部分显示这个对象的一些参数和说明，再下面的文本框中显示这个对象的值。当用户在树型结构中选择了某一对象，单击 Start 按钮，相应对象的值就会显示在这里。

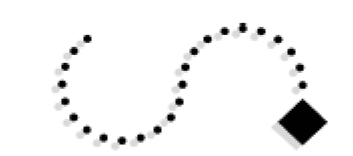
下面演示两个例子。第一个示例是查看 OID 为.iso.org.dod.internet.mgmt.mib-2.system.sysDescr 的对象的值，首先在树型结构中选择这个对象，单击 Start 按钮，列表框中就会出现如图 7-12 所示的内容。

第二个示例是查看 system 组中所有成员对象的值。首先选择对象.iso.org.dod.internet.mgmt.mib-2.system，单击 Start 按钮，列表框中就会出现如图 7-13 所示的内容。

3. 捕获和分析 SNMP 数据包

有了 Microsoft 网络监视器和 Getif 两个工具，捕获和分析 SNMP 数据包就非常容易了。首先启动 Microsoft 网络监视器并开始监听，然后启动 Getif，选择相应的 OID 对象，单击 Start 按钮，接着单击"Microsoft 网络监视器"窗口中的"停止并查看"按钮，打开如图 7-9 所示的捕获窗口，再双击相应的数据包就可以分析该数据包了。

下面举一个示例。假设要查看某一设备的 OID 为.iso.org.dod.internet.mgmt.mib-2.system.sysDescr 对象的值。按照上述步骤捕获了相应的数据包，如图 7-14 所示。



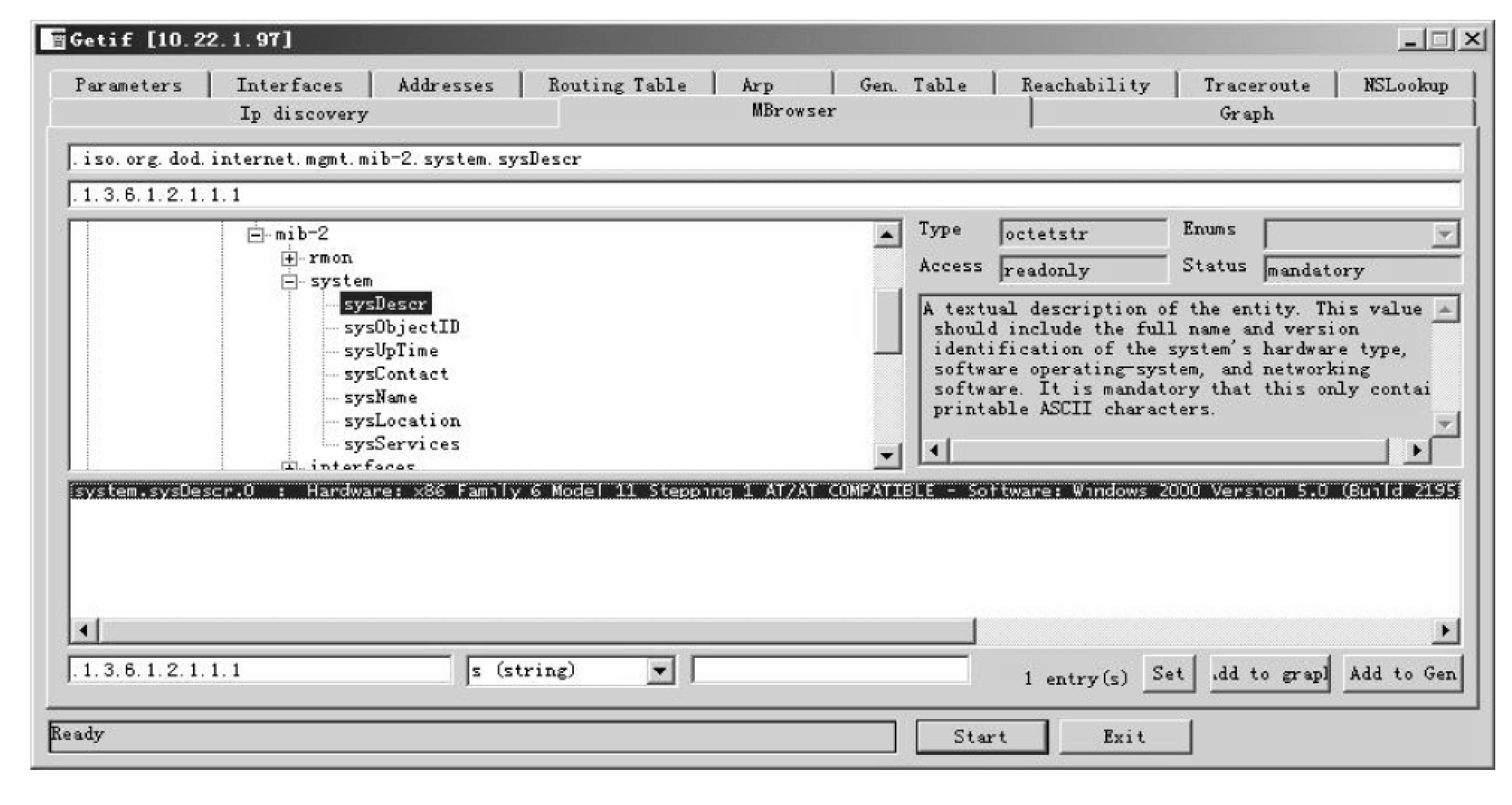


图 7-12　查看.iso.org.dod.internet.mgmt.mib-2.system.sysDescr 对象的值

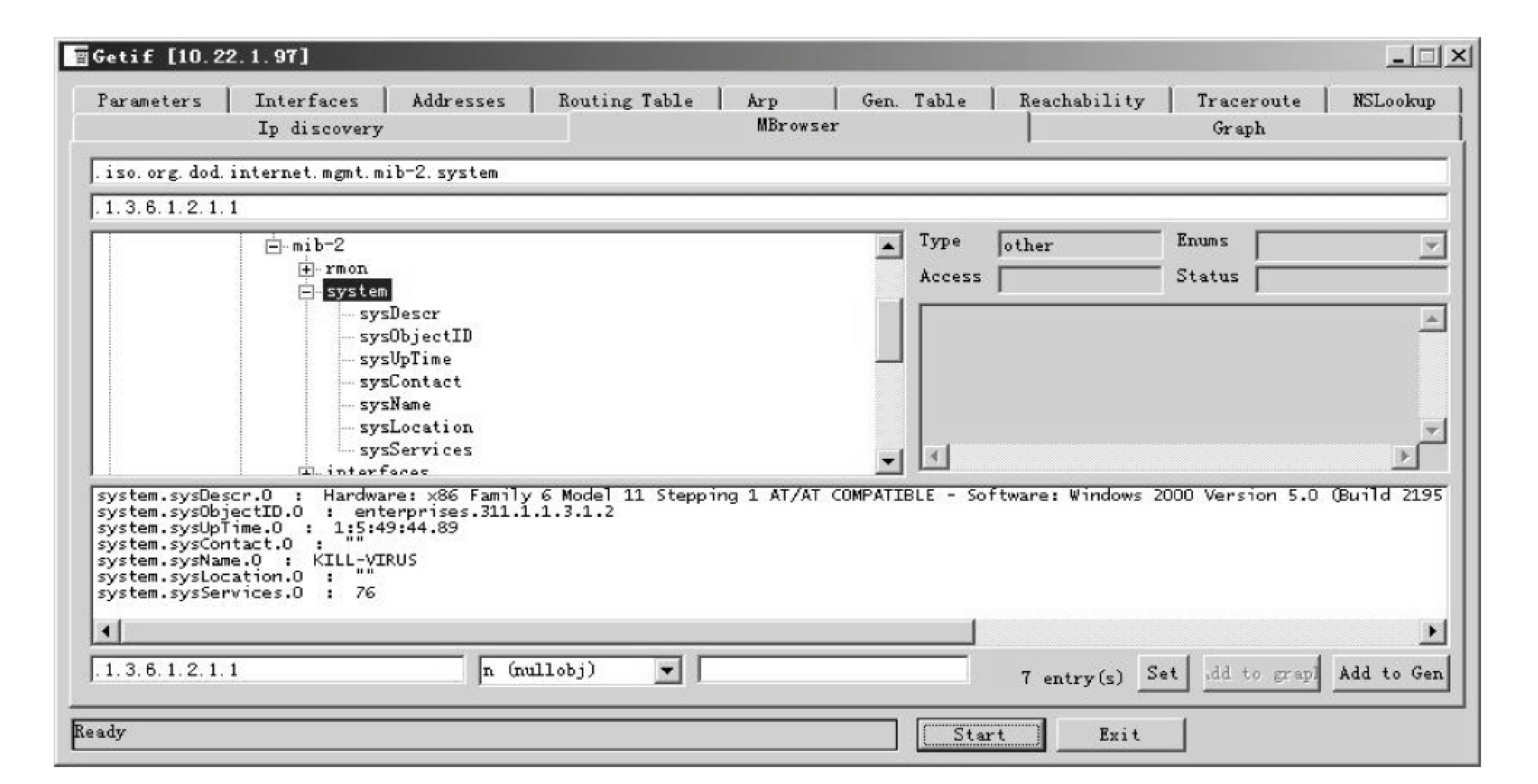


图 7-13　查看.iso.org.dod.internet.mgmt.mib-2.system 组中所有对象的值

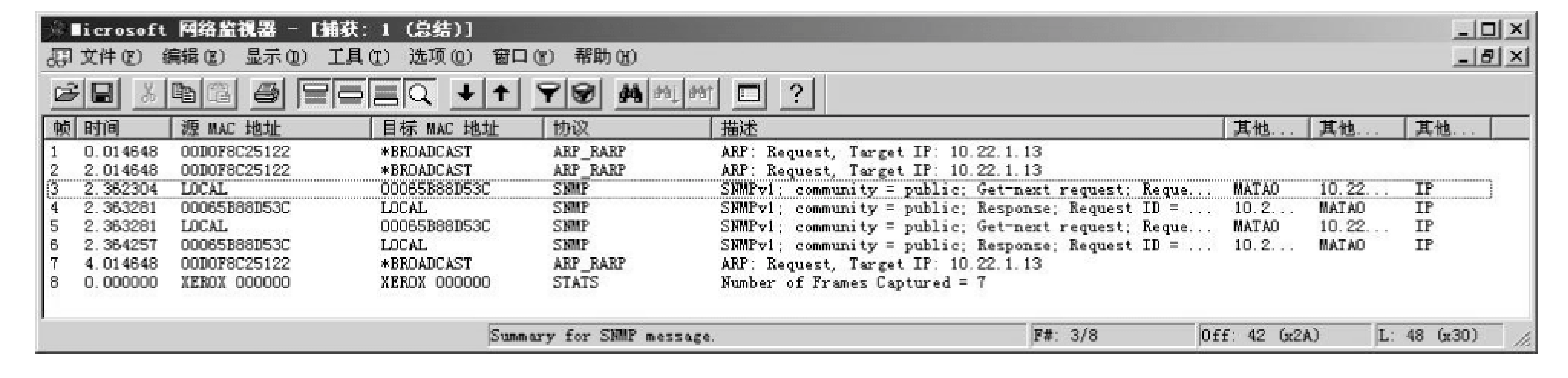


图 7-14　捕获数据包窗口

其中,第 3 个数据包是 SNMP 请求数据包,第 4 个数据包是 SNMP 应答数据包。双击第 3 个数据包,打开如图 7-15 所示的数据包分析窗口。

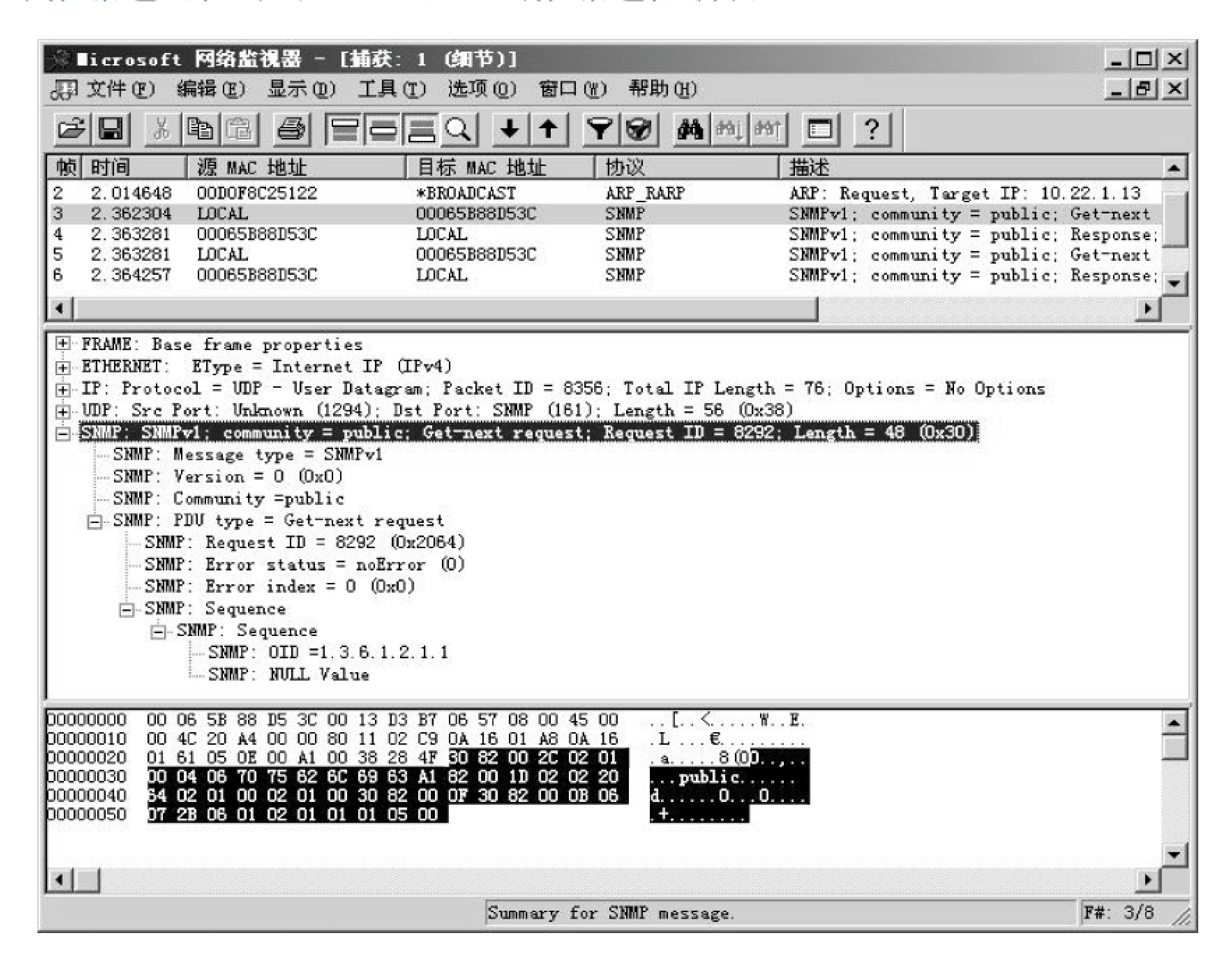


图 7-15 数据包分析窗口一

这个窗口分为 3 个部分,上面是捕获的数据包列表,中间是用户选中的数据包的分析情况,下面是数据包的十六进制表现形式。通过中间的数据包分析可以看到,SNMP 请求数据包分为 5 大部分:FRAME(数据包的全部数据)、ETHERNET(以太网数据头部分)、IP(IP 数据头部分)、UDP(UDP 数据报头部分)和 SNMP(SNMP 数据部分)。

下面分析一下 SNMP 的数据。

① Message type(SNMP 报文类型)。这个例子中 SNMPv1 对应的十六进制的值是 30,表示后面的数据是一个复合的构造类型。其后面的十六进制值 82 00 2C 表示这个 SNMP 数据部分去除前 4 个字节后的长度(44 个字节)。

② Version(SNMP 报文的版本号)。这个例子中 0 表示 SNMPv1。根据 ASN.1 转换语法,十六进制表现形式窗口中被选择的数据的第 5、6 和 7 字节表示版本号,其中 02 表示数据类型,01 表示数据长度,00 表示实际的值。

③ Community(共同体)。这里的值是 public,对应的十六进制是 04 06 70 75 62 6C 69 63,其中,04 表示是字符串数据,06 表示长度为 6 字节,其余表示实际的值。

④ PDU type(协议数据单元(PDU)的类型)。这里的值是 get-next request,对应的十六进制值是 a1。其他操作的值为,get-request 的值为 a0,get-response 的值为 a2。再后面的三个字节是 PDU 的头部,82 00 1D 表示后面还有 29 个字节的数据。

⑤ Request ID(请求标识)。数据包占 4 个字节,其中第一个 02 表示整型数据,第二个 02 表示数据长度,后面两个字节 2064 表示请求标识的值,即 8292。

⑥ Error status(差错状态),在请求时值设置为 0。十六进制表示为 02 01 00。

⑦ Error index(差错索引),在请求时值设置为 0。十六进制表示为 02 01 00。

⑧ Sequence。这里有两个 Sequence,都表示数据是集合类型。

⑨ OID(请求的 OID 对象名)。这里的值是 1.3.6.1.2.1.1。十六进制的值是 06 07 2b 06 01 02 01 01 01,其中第一个 06 数据是 MIB 变量名称类型,07 表示数据的长度,2b 表示 1.3 的和(即 1 * 40+3=0x2b)。

⑩ NULL Value(表示请求的 OID 对象的值)。请示时为空,十六进制的值是 05 00。

SNMP 请求数据包的响应包紧跟着被捕获,即第 4 个数据包。双击第 4 个数据包,打开如图 7-16 所示的数据包分析窗口。

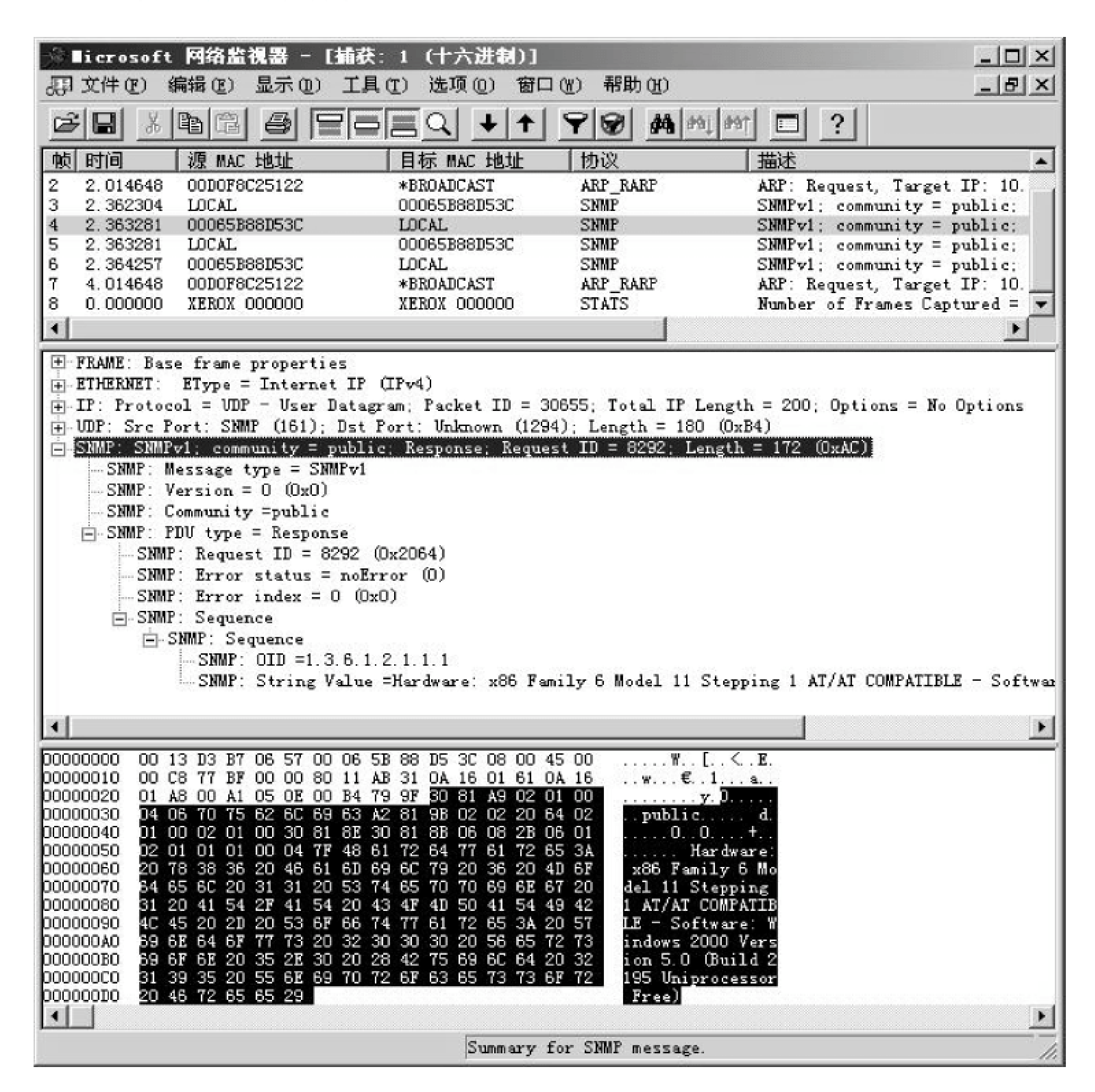


图 7-16　数据包分析窗口二

下面分析 SNMP 的数据:

① “Message type”:SNMP 报文类型。这个例子中“SNMPv1”对应的十六进制的值是“30”,表示后面的数据是一个复合的构造类型。再后面的十六进制值“81 A9”表示这个 SNMP 数据部分去除前几个字节后的长度(169 个字节)。

② “Version”：SNMP 报文的版本号。这个例子中是“0”，即表示为 SNMPv1。其十六进制对应的数据是“02 01 00”，其中“02”表示数据类型，“01”表示数据长度，“00”表示实际的值。

③ “Community”：共同体。这里的值是“public”，对应的十六进制是“04 06 70 75 62 6C 69 63”，其中“04”表示是字符串数据，“06”表示长度为 6 字节，其余表示实际的值。

④ “PDU type”：协议数据单元(PDU)的类型。这里的值是 get-response，对应的十六进制值是“a2”。再后面的两个字节是 PDU 的头部，“81 9B”表示后面剩余数据的长度。

⑤ “Request ID”：请求标识。这个值为 8292，同请求数据包中的值相同。

⑥ “Error status”：差错状态。这个例子中值为 0，表示没有错误。十六进制表示为“02 01 00”。

⑦ “Error index”：差错索引。这个例子中值为 0，表示没有错误。十六进制表示为“02 01 00”。

⑧ “Sequence”：这里有两个 Sequence，都表示数据是集合类型。

⑨ “OID”：请求的 OID 对象名。这里是 1.3.6.1.2.1.1。十六进制的值是“06 07 2b 06 01 02 01 01 01”，其中第一个“06”数据是 MIB 变量名称类型，“07”表示数据的长度，“2b”表示“1.3”的和(即 1 * 40+3=0x2b)。

⑩ “String Value”：表示请求的 OID 对象的值。

7.4 远程网络监视

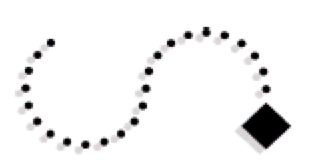
远程网络监控(RMON)是对 SNMP 的一个重要增强，对监测和管理网络特别有用。远程网络监控最大的优点就在于它与现存的 SNMP 框架相兼容，不需对 SNMP 进行任何修改即可使用。

7.4.1 RMON 的基本概念

远程网络监控(RMON)是一个标准监控规范，其本质上是 IETF 定义的一组对管理信息库(MIB-2)的功能的扩展，MIB-2 只提供单个设备的管理信息，而 RMON 可以使各种网络监控器和控制台系统之间交换网络监控数据，能够提供信息流量的统计结果和对网络参数进行分析，以便做出对网络的故障诊断、规划调整和性能控制。

RMON 监视系统由两部分构成：代理(监视器)和管理站。RMON 代理在 RMON MIB 中存储网络信息，代理可以被直接安装在网络设备中，也可以是在 PC 机上运行的一个应用程序。代理只能看到流经其自己的流量，所以在每个被监控的局域网网段或广域网链接点都要设置 RMON 代理。管理站用 SNMP 获取各个代理中的数据信息，汇总后形成整个网络系统的信息。

当前 RMON 有两种版本，分别是 RMON 和 RMON2。在目前使用较为广泛的网络硬件设备中都能发现 RMON，它定义了 9 个 MIB 组服务于基本远程网络监控；RMON2 是 RMON 的功能扩展，其主要针对数据链路层以上各 OSI 模型层进行监控。



1. 远程网络监视的目标

RMON 定义了远程网络监控的管理信息库，以及 SNMP 管理站和远程网络监视器之间的接口，一般 RMON 只是监视子网范围内的通信，从而减少管理者和代理之间的通信负担。RMON 具有下列目标。

① 离线操作。必要时管理者可以停止对监控器轮询，有限的轮询可以节省网络带宽和通信费用。即使不受管理者查询，监视器也要持续不断地收集子网故障、性能和配置方面的信息，统计和积累数据，以便管理者查询时能够及时提供相关的管理信息。另外，在网络系统出现异常情况时，监视器也能及时向管理者报告。

② 主动监视。如果监视器有足够的资源，通信负载也容许，监视器可以连续性地或周期性地运行诊断程序，查询并记录网络系统的性能参数，在子网出现失效时通知管理者，给其提供有效的诊断故障信息。

③ 问题检测和报告。如果主动监视消耗网络资源太多，监视器也可以被动地获取网络数据，可以配置监视器，使其连续观察网络资源的消耗情况，记录随时出现的异常事件，并在出现错误事件时通知管理者，以便管理者做出相应的反应。

④ 提供增值数据。监视器可以分析收集到的子网数据，从而减轻管理者的计算任务。

⑤ 多管理站操作。一个互联网可能有多个管理站，这样可以提高可靠性，或是分布地实现各种不同的网络管理功能。监视器可以配置为并发的工作模式，为不同的管理站提供不同的信息。

注意：不是每一个监视器都能实现上述所有目标，RMON 的规范只是提供了实现这些目标的基础结构和理论依据。

2. 表管理操作原理

在 SNMPv 管理框架中，对表操作的规定很不完善，增加和删除表行的操作是不明确的。这种模糊性常常是用户提问的焦点和抱怨的根源。RMON 规范包含了一组文字约定和过程规则，在不修改、不违反 SNMP 管理框架的前提下，提供了清晰准确并有规律性的行增加和行删除操作。

3. 多管理站访问

RMON 监视器应允许多个管理站并发访问，当多个管理站同时访问时可能出现下列问题：

① 多个管理站对资源的并发访问可能超过监视器的能力；

② 一个管理站可能长时间占用监视器资源，使得其他管理站无法访问；

③ 占用监视器资源的管理站可能发生崩溃，但是其没有释放占用的资源。

对于上述问题，RMON 提出了解决问题的方法：

① 管理站能认得自己所属的资源，也知道自己不再需要的资源；

② 网络管理操作员可以知道管理站占有的资源，并决定是否释放这些资源；

③ 一个被授权的网络操作员可以单方面决定是否释放其他操作员所占用的资源；

④ 如果管理站经过了重启动过程，应该首先释放不再使用的资源。

7.4.2 RMON的信息管理库

RMON MIB由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。RMON规范定义了管理站信息库RMON MIB，它是MIB-2下面的子树，其OID为.iso.org.dod.internet.mgmt.mib-2.rmon(.1.3.6.1.2.1.16)。RMON MIB共分为9个组，存储在每一组中的信息都是监视器从一个或几个子网中统计和收集的数据。这9个组分别是

① 统计量组(Statistics)：提供了一个以太网状态表，标志子网的统计信息，大部分是计数器。

② 历史组(History)：存储通过固定间隔取样所获得的子网信息数据，其由历史控指标和以太网历史表组成。

③ 报警组(Alarm)：由一个表组成，该表定义了监视的变量、采样区间和阈值。报警类型有两种：absolutevalue(1)表示直接与阈比较；datavalue(2)表示相减后比较校正量报警。

④ 主机组(Hosts)：收集新出现的主机信息，内容与接口组同。

⑤ 主机最大值组(Host Top N)：记录某组参数最大的N台主机的有关信息，信息来源于主机组。

⑥ 矩阵组(Matrix)：记录子网中主机之间的通信量，信息以矩阵形式存储。

⑦ 过滤器组(Filter)：通过过滤选择出某种指定的特殊分组，这个组定义了两个过滤器：数据过滤器按位模式匹配；状态过滤器按状态匹配。

⑧ 捕获组(Capture)：建立一组缓冲区，用于存储从通道中捕获的分组，其由控制表和数据表组成。

⑨ 事件组(Event)：其作用是管理事件，由事件表和log表组成，前者定义事件的作用，后者记录时间出现的顺序。事件是由MIB中其他地方的条件触发的，事件也能触发其他地方的作用。产生事件的条件在RMON其他组中定义，如报警组和过滤组都可以指向事件组的索引项。时间还能使事件组存储有关信息，甚至引起代理进程发送陷入消息。

RMON组的组成图如图7-17所示。一般的交换机至少支持4组(即统计量组、历史组、报警组和事件组)。

这9个功能组都是任选的，但实现时有下列关联关系：

① 实现警报组时必须实现事件组。

② 实现主机最大值组时必须实现主机组。

③ 实现捕获组时必须实现过滤组。

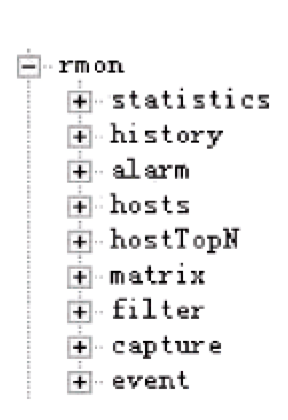
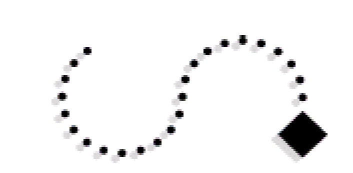


图7-17 RMON组的组成图

7.4.3 RMON2信息管理库

RMON主要监测和控制OSI模型中的物理层和数据链路层，而ROMN2主要应用于OSI模型中数据链路层以上各层，主要监控IP流量和应用程序层流量。RMON2允许网络管理应用程序监控所有网络层的信息包，这与RMON不同，RMON只允许监控数据链路层及其以下层的信息包。

RMON2监视OSI模型中第3层到第7层的通信数据，能够对数据链路层以上的分



组进行译码，这使得监视器可以管理网络层以上协议，包括 IP 协议，因而能了解分组的源和目标地址，能知道路由器负载的来源，使得监视的范围扩大到局域网之外。监视器也能监视应用层协议，如电子邮件协议、文件传输协议、HTTP 协议等，这样监视器就可以记录主机应用活动的数据，显示各种应用活动的图表，这些数据和图表对网络管理人员来说都是很重要的信息。

RMON2 在 RMON MIB 基础上增加了 9 个功能组。

① 协议目录组：提供各种网络协议的标准化方法，使得管理站可以了解监视器所在子网上运行什么协议。协议目录是一种简单的便于共同建立 RMON2 应用程序、实现 RMON 代理的途径，这对于应用程序和代理出自不同的提供商的情况尤其重要；

② 协议分布组：提供每个协议产生的通信统计数据，将监测器收集的数据转换为正确的协议名，从而可以显示给网络管理者；

③ 地址映像组：IP 地址与 MAC 地址的映射表。MAC 层的地址与网络层的地址之间的转换使读和记忆变得容易，地址转换不仅为网络管理者提供了帮助，而且支持 SNMP 管理平台并引入了改进的拓扑布局转换；

④ 网络层主机组：收集网络上主机的信息；

⑤ 网络层矩阵组：统计网络上源和目标的通信情况；

⑥ 应用层主机组：收集每个应用的通信情况；

⑦ 应用层矩阵组：统计应用协议之间的通信情况；

⑧ 用户历史组：周期性地收集统计数据，使网络管理者能够配置系统中的任何历史记录，例如，在指定文件服务器或路由器对路由器的连接上的特殊历史记录；

⑨ 监视器配置组：定义了监视器的标准参数的集合，使某提供商的 RMON 应用程序能够配置其他提供商的 RMON 探测器。

RMON2 还引入了两种与对象索引有关的新功能：外部对象索引和时间过滤器索引，增加了 RMON2 的能力和灵活性。

7.5　本章小结

本章主要讲述了基于简单网络管理协议（SNMP）的网络管理内容和管理信息库（MIB）的概念及组成，重点讲解了 SNMP 协议数据单元和其操作功能，并给出了一些示例，最后对远程网络监控（RMON 和 RMON2）进行了简单的讲解。因为学时限制，在教材中没有介绍 SNMP 的全部内容，感兴趣的读者可以参阅其他教材。

7.6　本章习题

1. 根据 ISO 定义的网络管理有哪几个功能？
2. 管理信息库第 2 版（MIB-2）中有 9 个功能组，分别是什么？
3. 简单网络管理协议（SNMP）有哪几个操作？
4. 远程网络监控（RMON）的功能是什么？

第 8 章

网络管理软件

本章内容：

本章没有承接第 7 章介绍基于 SNMP 协议的网络管理软件，是缘于本课程的网络使用环境为小型的局域网，因此重点介绍了功能相对比较简单的网路岗软件的使用方法和技巧。

本章重点：

① 了解网络管理软件的种类。

② 掌握网路岗管理软件的安装、设置、管理、使用方法与技巧。

③ 了解 NAT 的基本概念。

随着计算机网络日新月异的迅猛发展，网络管理软件也大量地涌现出来，有的网络管理软件非常专业，针对某一方向可以实现颗粒度很细的管理，如基于 SNMP 协议的 CISCO works、HP OPENVIEW 等，这些软件主要应用在对监控要求较高的计算机网络中。在一般的计算机网络中，考虑到成本、网络规模和使用要求，并不需要安装这样专业的管理软件，安装功能比较丰富、操作比较方便的一般网络管理软件就可以了。本章要介绍的网路岗软件是一款应用比较广泛的网络监控产品，自 2002 年推出第一代产品以来，通过不断的完善与改进，现在已经升级到第五代，在产品监控功能不断增强的同时，产品的稳定性也得到大幅度提高，得到了广泛的应用。特别说明：安装和使用网路岗软件请参考网路岗第五代使用手册。

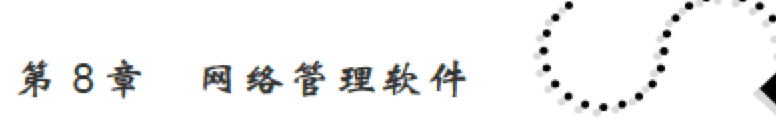
8.1 网路岗软件的安装与验证

8.1.1 软件的安装

1. 系统要求

(1) 操作系统为 Windows XP/2000/2003 以上。

(2) CPU 为 Pentium 4 或赛扬 2.0Gbps 以上。



（3）硬盘的空闲空间不低于 10Gbps。

2. 安装步骤

（1）打开安装光盘，运行安装主监控程序 Sentry5Corp. exe。

（2）主程序安装完毕后，安装光盘中的网路岗驱动程序 SentryDrv. exe。

提示：按默认选项操作即可安装成功。

特别说明：

ETC\子目录存放与系统有关的所有配置文件；

PcInfo. map 是基于网卡网络监控模式的信息；

UserInfo. map 是基于账户网络监控模式的信息；

IpInfo. map 是基于 IP 网络监控模式的信息；

ShareArea. map 存放的是系统配置数据；

CapLog\是系统默认的用来存放监控日志的目录；

CapLog\Activities\存放的是网络活动日志；

CapLog\WebFiles\存放的是外发资料日志。

（3）完成安装，运行网路岗软件出现的界面，如图 8-1 所示。



图 8-1　网路岗界面

3. 软件配置

（1）绑定网卡（如图 8-2 所示）

绑定网卡就是选择从哪块网卡抓信息包。

绑定网卡的注意事项：

① 若安装网路岗的计算机有多块网卡，则选择网卡时要谨慎，选错网卡，网路岗不但监视不了任何信息，也不能对目标机器进行任何控制。



图 8-2　绑定网卡

② 选择网卡时，应选择内网段的网卡，而不能选择接入因特网的网卡。

提示：默认情况下，系统获取通信数据包的网卡和发送封堵包的网卡是同一块，但特殊情况下可以设置信息过滤网卡，以便系统通过另外一块网卡来发送封堵包以控制目标机器。

有一种情况必须启用信息过滤专用网卡，即设置镜像端口来实现对数据包监视后，却不能和局域网其他机器进行通信（假定该机器 IP/网关配置正确），也就是说，所设置的镜像端口只能接受信息包，而不能发送数据包，镜像端口是单向的。针对这类情况，建议再添一块网卡，作为网路岗的信息过滤专用网卡。

在网路岗界面中单击“高级设置”按钮，弹出“高级设置”对话框，如图 8-3 所示，在该对话框中设置信息过滤专用网卡。配置时必须注意，信息过滤网卡的镜像端口和被镜像端口必须在同一交换机的同一 VLAN 中。

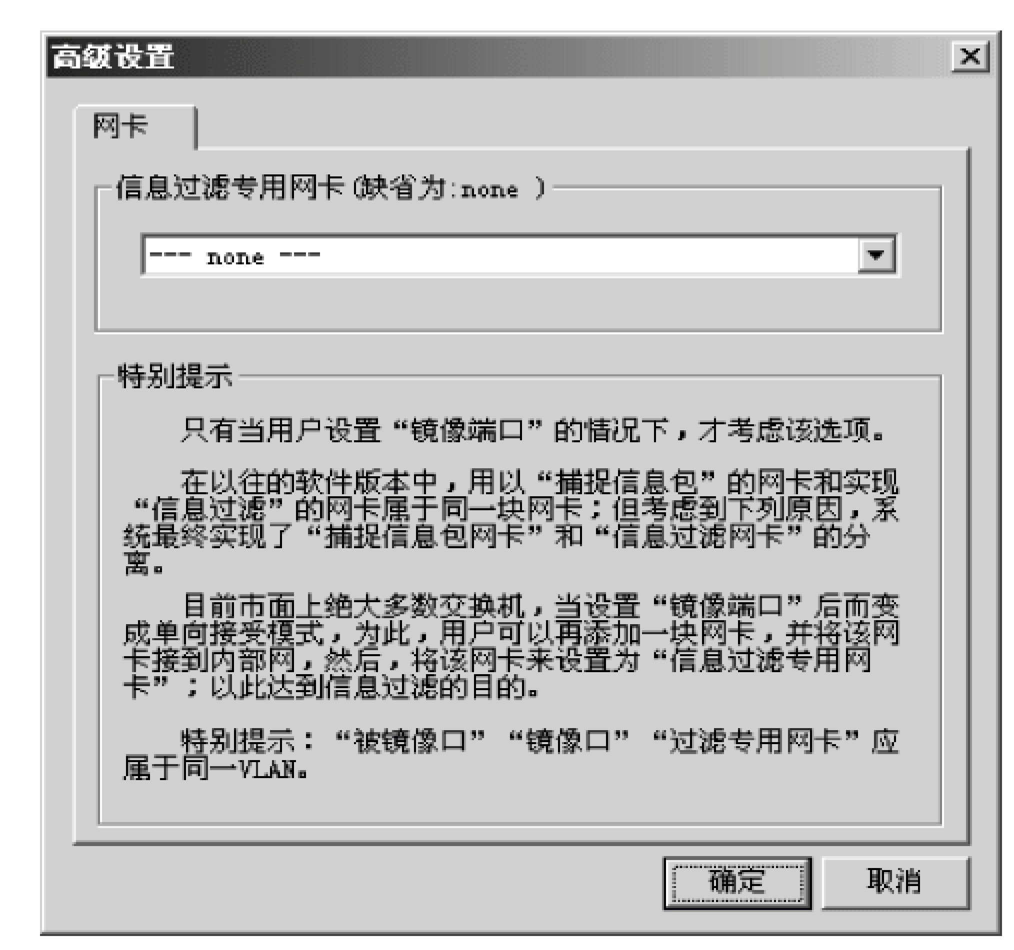


图 8-3　“高级设置”对话框

（2）查看监控效果

测试监控效果时，在网路岗界面的工具栏中单击“现场观察”按钮，打开“现场观察”窗口，先观察能否实时监控到目标机器上网页面的情况。

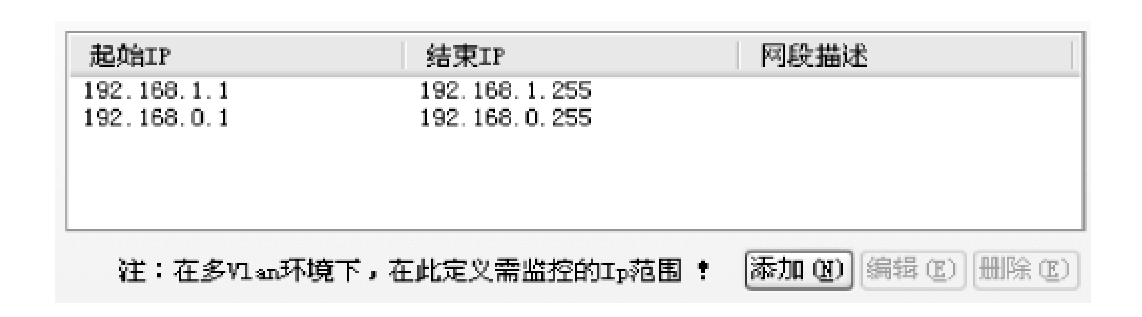
单击“服务”选项，双击要启动服务的图标，启动所有的后台监控服务，如图 8-4 所示。



图 8-4　后台监控服务图标

（3）配置内部网段

单击“网络定义”选项，在弹出的对话框的“内部网 IP 范围”选项组中，如图 8-5 所示。设置起始 IP 及结束 IP。这里需要提醒的是：只有监控多个子网时，才需要手动配置内部网 IP 范围。



起始IP	结束IP	网段描述
192.168.1.1	192.168.1.255	
192.168.0.1	192.168.0.255	

图 8-5　内部网 IP 范围设置

8.1.2　验证安装是否正确

（1）检查目标机器的监控状态

单击“基于网卡模式”选项，先看看是否有机器信息，如果没有，单击“搜索邻居”按钮试着搜索每台机器，单击某台机器前的小图标，该机器的状态可循环改变，如图 8-6 所示。

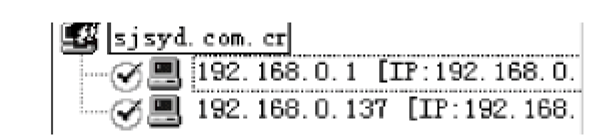


图 8-6　目标监控状况

其中表示该机器被监控，vip表示该机器不被监控，表示该机器不被监控但也不允许上网。



图 8-7　“封堵端口”选项卡

（2）检查被监控机器的上网情况

选择“文件”→“现场观察”命令，在确保被测试的机器处于状态后，让该机器上网，比如 www.google.com 等，并留意“现场观察”窗口中是否有对应的信息；如果该窗口中能正确显示目标机器的上网情况，说明对该机器的监控是正常的，而对该机器的封堵也将起作用。

（3）封锁目标机器上网

选中被测试的机器，打开“封堵端口”选项卡，如图 8-7 所示。

选择 80 端口（注：如果网络采用代理上网，则上网端口可能不是 80，则需要添加新的端口，并选择该窗口），封锁时间段全绿，单击“更新规则＝＞ET”按钮，最后单击“保存设置”按钮使设置生效。

设置完毕，再次让目标机器上网，并检查“现场观察”窗口中的记录显示。

通过上述 3 个步骤的测试，可以有效地检测网路岗软件安装是否成功。

8.2　网路岗各种监控模式的介绍

8.2.1　基于网卡监控

基于网卡监控就是以网卡 MAC 为依据，根据网卡 MAC 地址确定被监控的信息的身份。由于每台机器的网卡 MAC 相对固定，被监控的机器不易修改，因此建议管理员将

该网络监控模式列为首选。

在基于网卡网络监控模式下，被监控的机器更换新的网卡后，网路岗会检测到新的网卡 MAC，因此，新网卡将被当作新加入的机器来处理，在此提醒管理员注意。

基于网卡网络监控模式的操作步骤如下：

（1）选择网络监控模式。在“当前监控模式”下拉列表框中选择“1. 基于网卡 MAC”，如图 8-8 所示。

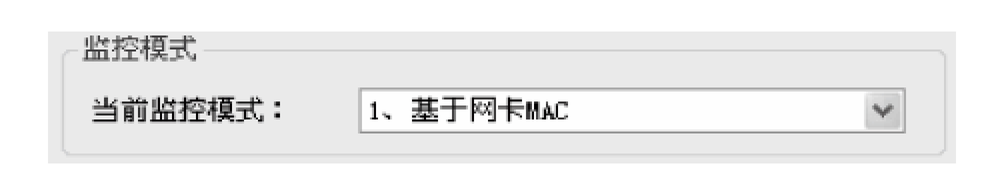


图 8-8　选择网络监控模式

（2）设置监控对象，如图 8-9 所示。

下面介绍界面操作按钮的功能。



图 8-9　设置监控对象

“搜索邻居”：自动探测指定 IP 范围内的机器信息（IP 地址/网卡 MAC）。

“新组”：创建新的群组，以便对目标机器进行分组管理。

“转移”：将选中的机器转移到其他部门，也可以直接用鼠标指针将目标机器从一个部门拖到另外一个部门。

“编辑”：改变某一选中机器的机器名称或改变群组名称。

“删除”：删除选中的一个或多个目标，也可用来删除空的群组。

“查找”：如果目标机器太多，可以用此功能来找出要找的机器。

“解析”：当新机器被加入时，机器名默认为其 IP 地址，如想将 IP 地址转变成机器名，可使用此功能。

“导出”：将目标机器的信息及其对应的规则配置导出到自定义的文件中。

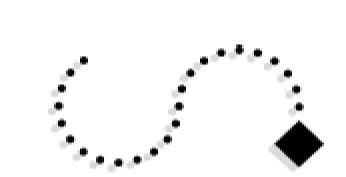
“导入”：将导出的机器及规则配置信息从指定的文件加入到当前机器列表中。

“保存设置”：保存对目标机器信息/群组信息/上网规则等信息的改动。

改变目标机器的排序方式。选中“搜索邻居”按钮上方的 3 个 Option 单选按钮，可分别以机器名/IP 地址/MAC 的排序方式显示目标机器。

单选/多选目标机器。单击目标机器，可以选择单一目标；按下鼠标左键并拖动，可以多选目标，也可同时按下鼠标左键和 Shift/Ctrl 键进行多选。

双击目标机器后，将弹出编辑机器名称“对话框”。



更改目标机器监控状态。在目标机器的状态小图标上单击，可改变其监控状态。

如果图 8-9 左边部分为空，则需要先启动监控服务，选择绑定正确的网卡，然后单击“搜索邻居”按钮，弹出“目标搜索”对话框，输入正确的 IP 范围，单击“开始搜索”按钮，开始搜索。

在“发现新机器”选项组中选中“立即加入”单选按钮，如果有机器上网，新发现的机器可以自动加入；每一目标机器都有相应的目录，默认情况下，新机器都放入目录 New Folder 中。

8.2.2　基于 IP 监控

基于 IP 监控是以 IP 地址为依据，并以此 IP 来确定所监控的信息的身份。

当群十分庞大的时候，在基于 IP 监控的方式下，管理员可定义一个 IP 范围段来作为一个管理对象。管理员可能只关心某一范围内机器的上网情况，以便对这些机器进行统一的控制，不一定非要具体到某台机器。

基于 IP 网络监控模式的操作步骤如下。

（1）选择基于 IP 的网络监控模式。在“当前监控模式”下拉列表框中选择“3. 基于 IP”，如图 8-10 所示。

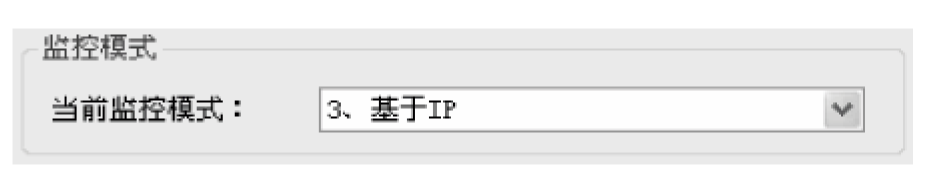


图 8-10　选择网络监控模式

（2）设置监控对象，如图 8-11 所示。

下面介绍界面操作按钮的功能。

“搜索邻居”：自动探测指定 IP 范围内的机器信息（IP 地址/网卡 MAC）。

“新组”：创建新的群组，以便对目标机器进行分组管理。

“转移”：将选中的机器转移到其他部门，也可以直接用鼠标指针将目标机器从一个部门拖到另外一个部门。

“编辑”：改变选中机器的 IP 地址/描述或改变群组名称。

“删除”：删除选中的一个或多个目标，也可用来删除空的目录。

“查找”：如果目标机器太多，可以用此功能来找出要找的机器。

“解析”：当新机器被加入时，机器名默认为空，如想得到机器名，可使用此功能。

“导出”：将目标机器的信息及其对应的规则配置导出到自定义的文件中。



图 8-11　设置监控对象

“导入”：将导出的机器及规则配置信息从指定的文件加入到当前机器列表中。

“保存设置”：保存对目标机器信息/群组信息/上网规则等信息的改动。

单选/多选目标机器。单击目标机器，以选择单一目标；按下鼠标左键并拖动，以多选目标，也可用鼠标左键配合 Shift/Ctrl 键进行选择。

双击目标机器后，将弹出“编辑机器名称”对话框。

更改目标机器监控状态。在目标机器的状态小图标上单击，可改变其监控状态。

如果图 8-11 左边部分为空，则需要先启动监控服务，选择绑定正确的网卡，然后单击“搜索邻居”按钮，弹出“目标搜索”对话框，输入正确的 IP 范围，单击“开始搜索”按钮，开始搜索。

在“发现新机器”选项组中选中“立即加入”单选按钮，如果有机器上网，新发现的机器可以自动加入；每一目标机器都有相应的目录，默认情况下，新机器都放入目录 New Folder 中。

8.2.3 基于账户监控

账户模式又分为两种情况。

- 活动目录（域）情况。采用此网络监控模式的前提是，在网络内安装并启用了活动目录，上网用户需要先通过域登录才可以访问互联网资源；每个上网用户都有自己的账户和密码，一个账户可在多台机器上登录。针对这类情况，网路岗没有必要重新定义一套账户来管理上网，只需要从活动目录中获取账户信息，通过现有的账户管理上网即可。
- 系统自定义情况（多在网吧中使用）。在此网络监控模式下，目标机器首次上网时，如访问外部网站，在 IE 窗口中将会出现要求身份验证的对话框，当验证通过后，在屏幕上方自动弹出计时窗口，表明目标机器的在线情况，这时候，目标机器才可以正常上网、收发邮件等。

1. 额外的配置

采用基于账户的网络监控模式，要求在监控机上安装 Microsoft IIS 组件，该组件附带在 Windows 2000/XP/2003 等专业版/服务器版的安装光盘中。IIS 安装设置步骤如下：

（1）安装 IIS

打开“控制面板”窗口，双击“添加/删除程序”图标，在“添加/删除程序”窗口中单击“添加/删除 Windows 组件”图标，在“Windows 组件向导”对话框中检查“Internet 信息服务（IIS）”复选框是否被选中，如没有选中，请选择它，并单击“下一步”按钮开始安装 IIS。

（2）配置 IIS

安装完成后，需要对 IIS 进行配置，具体步骤如下。

① 打开“控制面板”窗口，单击“管理工具”图标，在“管理工具”窗口单击“Internet 信息服务”图标，打开“Internet 信息服务”窗口，如图 8-12 所示。

② 右击“默认 Web 站点”，在弹出的快捷菜单中选择“属性”命令，弹出“默认 Web 站点属性”对话框，如图 8-13 所示。

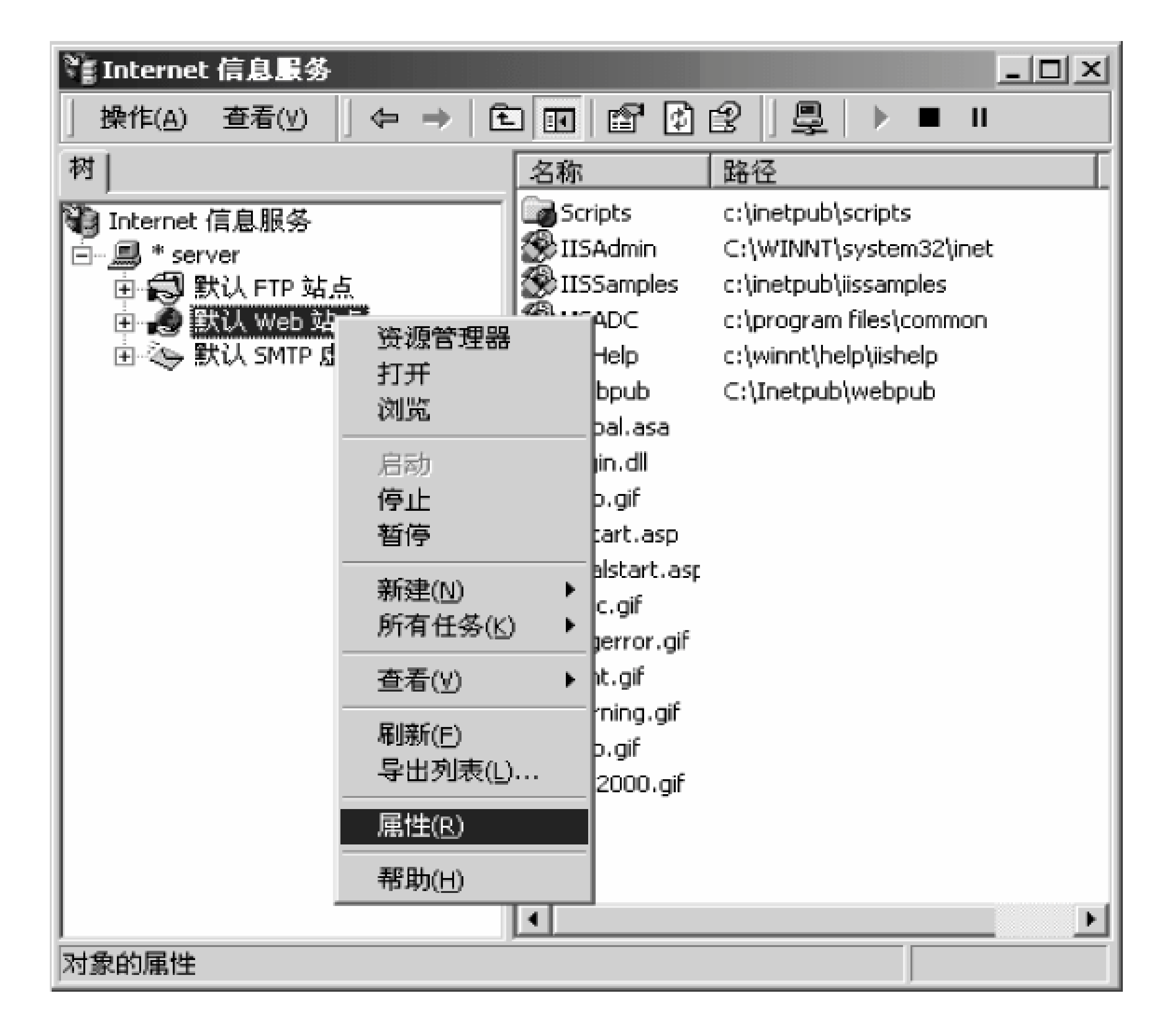


图 8-12　“Internet 信息服务”窗口

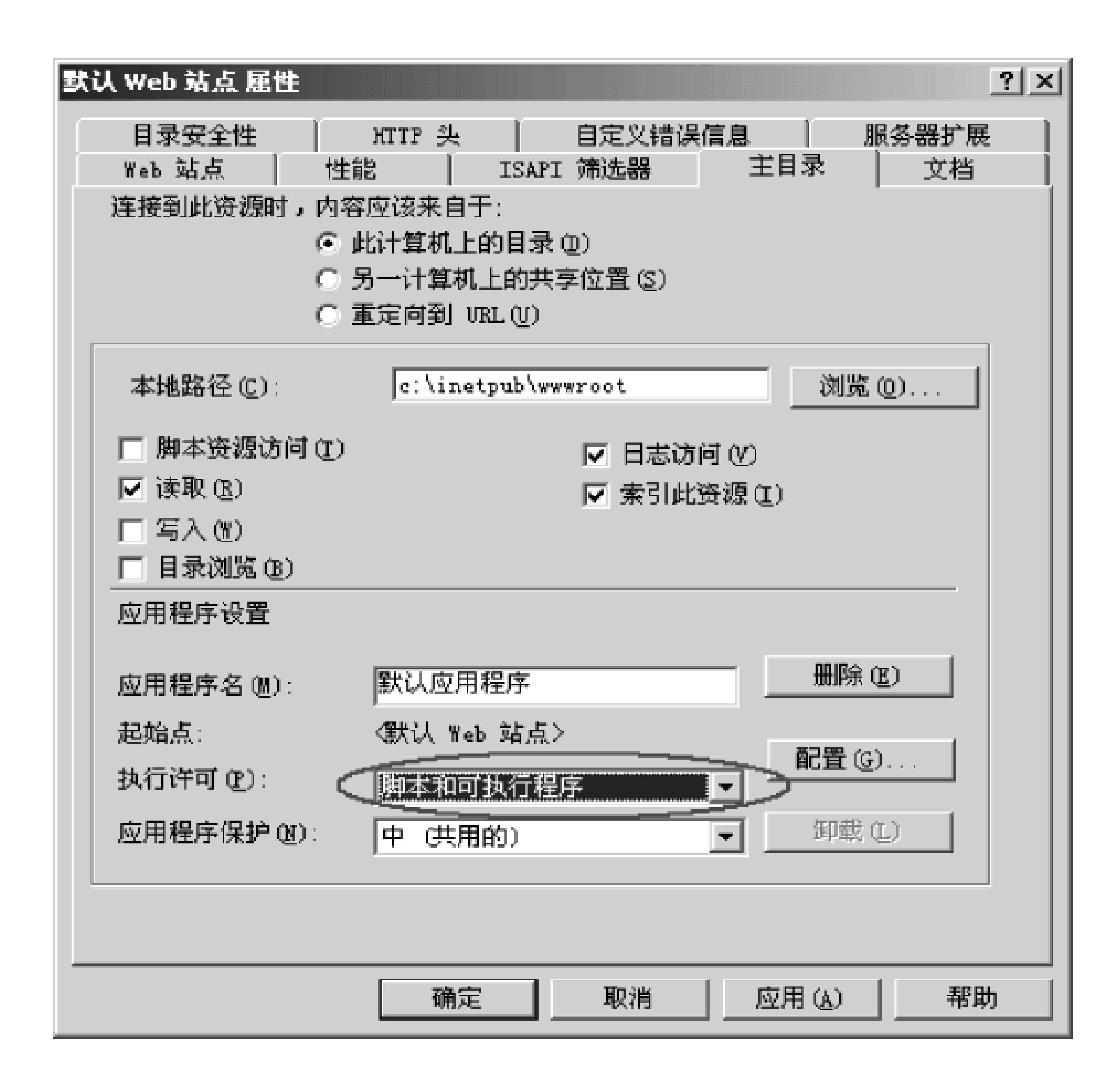


图 8-13　“默认 Web 站点属性”对话框

③ 打开“Web 站点”选项卡，在“执行许可”下拉列表框中选择“脚本和可执行程序”，单击“确定”按钮，配置执行许可权限。

(3) 将 Login.dll 复制到正确位置。从光盘的安装程序目录下复制 Login.dll 文件到 wwwroot 目录，如图 8-14 所示。完成 IIS 的安装和配置。

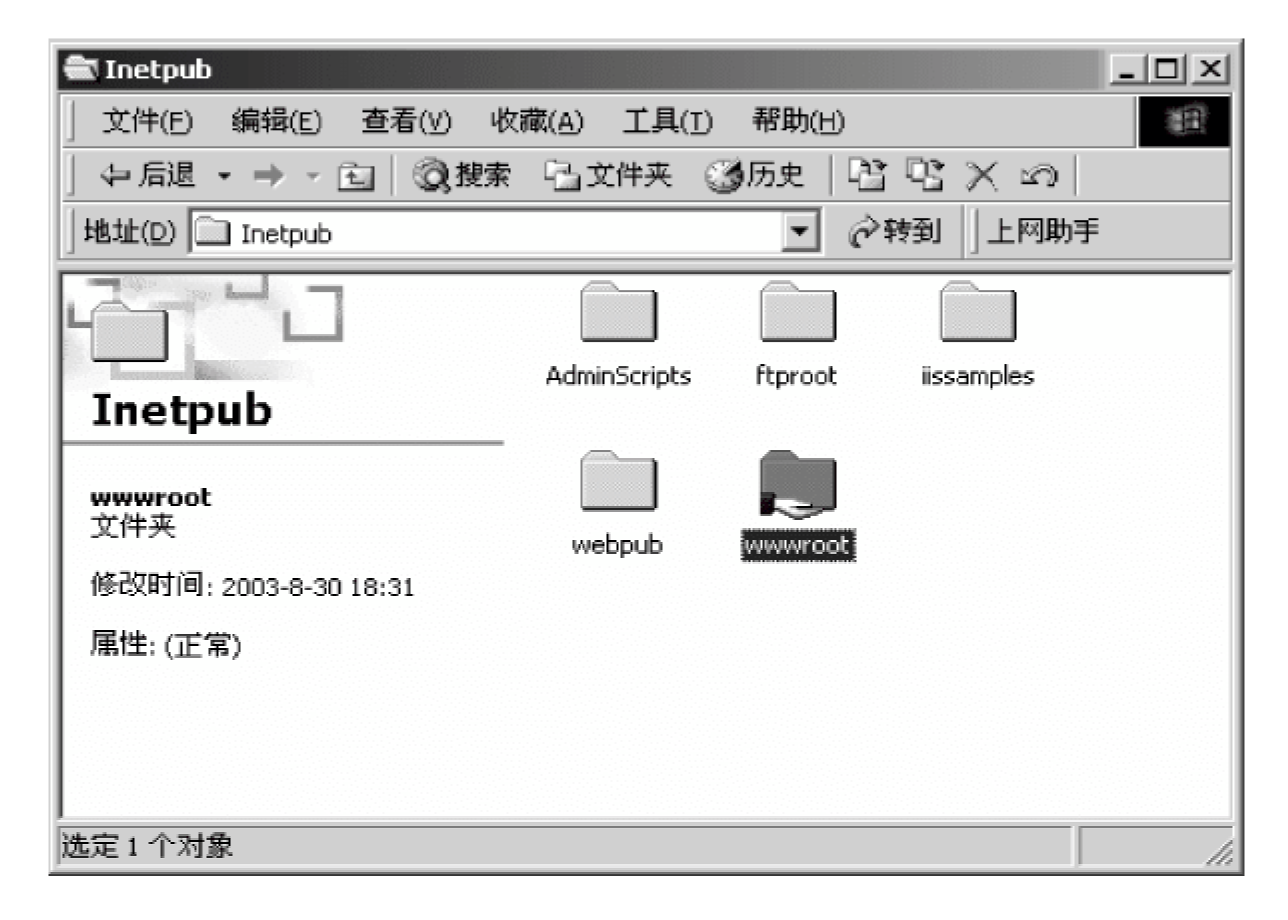


图 8-14 根文件夹

2. 基于账户网络监控模式的实施

(1) 选择基于账户的网络监控模式。在“当前监控模式”下拉列表框中选择“2. 基于账户”,如图 8-15 所示。

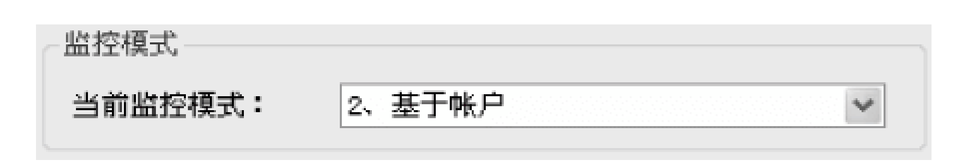


图 8-15 选择监控模式

(2) 设置监控对象,如图 8-16 所示。

单击“验证 Url”按钮,弹出“设置验证地址”对话框,在该对话框中输入网路岗扩展库 Login. dll 的访问地址 http://192.168.0.237/login.dll,如图 8-17 所示。

192.168.0.237 是监控机,且该机器上安装了 Microsoft IIS,如果一切配置正常,单击“测试”按钮后,在 IE 窗口中会显示如下信息:Testing Login. dll...OK. 。

下面介绍界面操作按钮的功能。

“新组”:创建新的群组,以便对账户进行分组管理。

“转移”:将选中的账户转移到其他部门,也可以直接用鼠标指针将账户从一个部门拖到另外一个部门。

“编辑”:改变某一选中账户信息或改变群组名称。

“删除”:删除选中的一个或多个账户,也可用来删除空的目录。

“查找”:如果账户太多,可以用此功能来找出要找的账户。

“解析”:当新机器被加入时,机器名默认为空,如想得到机器名,可使用此功能。

“导出”:将账户的信息及其对应的规则配置导出到自定义的文件中。

“导入”:将导出的账户及规则配置信息从指定的文件加入到当前账户列表中。

“保存设置”:保存对账户信息/群组信息/上网规则等信息的改动。

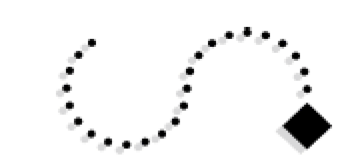





图 8-16 设置监控对象

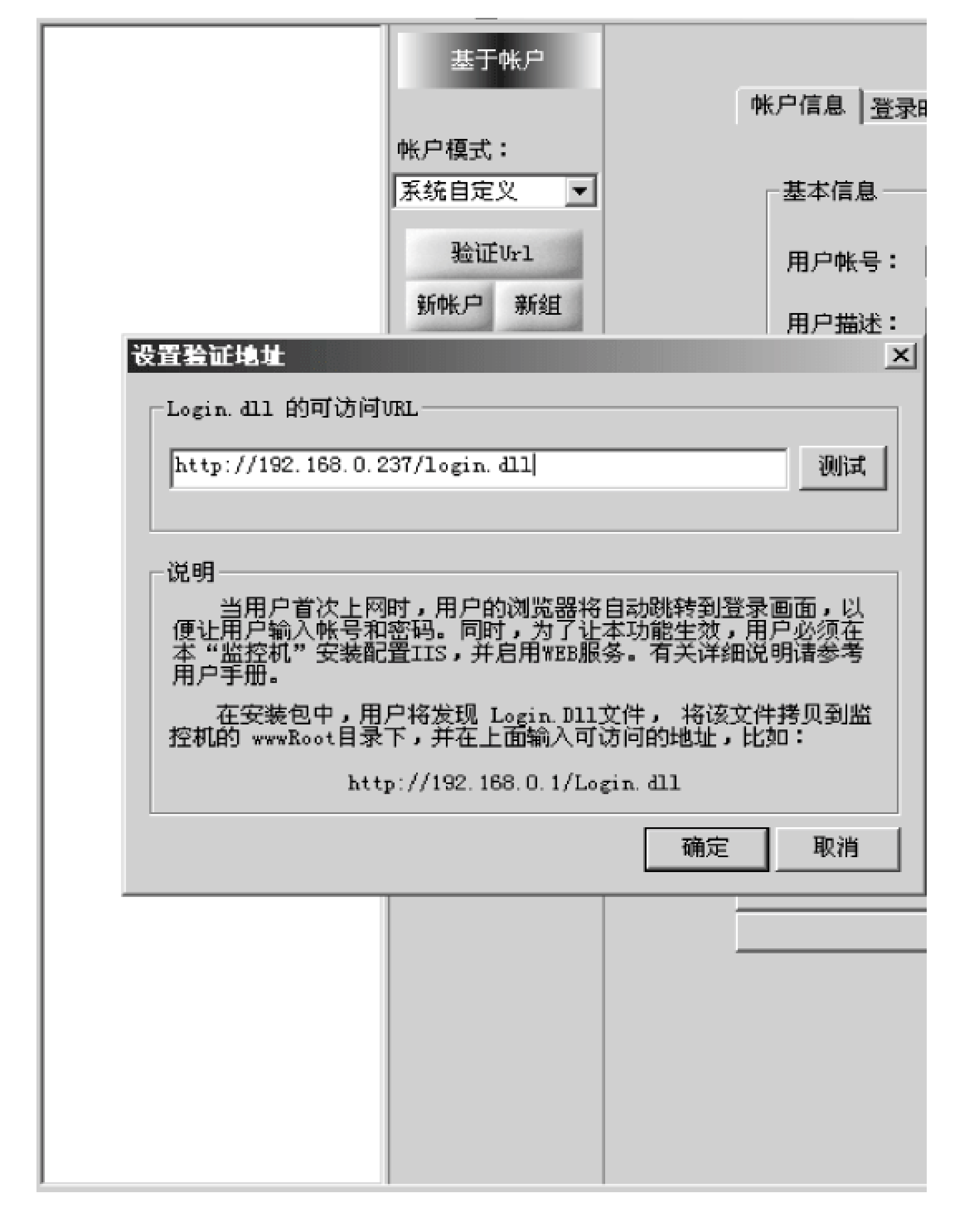


图 8-17 设置验证地址

单选/多选账户。单击账户，以选择单一目标；按下鼠标左键并拖动，以多选目标，也可用鼠标左键配合 Shift/Ctrl 键进行选择。

双击账户后，将弹出编辑窗口。

更改账户监控状态。在账户的状态小图标上单击，可改变其监控状态。

8.3 NAT 功能和常见配置

8.3.1 NAT 功能

1. 有关 NAT 的介绍

（1）NAT 的基本知识

网络地址转换（NAT）是一个因特网工程任务组（Internet Engineering Task Force，IETF）标准，允许专用网络上的多台 PC（使用专用地址段，例如 10.0.x.x、192.168.x.x、172.x.x.x）共享单个或全局路由的 IPv4 地址。IPv4 地址日益不足是部署 NAT 的一个主要原因。Windows XP 和 Windows Me 中的“Internet 连接共享”及许多 Internet 网关设备都使用 NAT，尤其是在通过 DSL 或电缆调制解调器连接宽带网的情况下。

NAT 对于解决 IPv4 地址耗费问题（在 IPv6 部署中却没必要）尽管很有效，但毕竟属于临时性的解决方案。IPv4 地址占用问题在亚洲及世界其他一些地方已比较严重，且日

渐成为北美地区需要关注的问题,这就是人们长久以来一直使用 IPv6 来克服这个问题的原因所在。

除了减少所需的 IPv4 地址外,由于专用网络之外的所有主机都通过一个共享的 IP 地址来监控通信,因此 NAT 还为专用网络提供了一个隐匿层。NAT 与防火墙或代理服务器不同,但它确实有利于安全。

(2) 网路岗 NAT 适用环境

① 双网卡:一个接因特网,一个接内网。

② 单网卡+电话线拨号。

③ 单网卡+ADSL Modem。

(3) 网路岗 NAT 功能介绍

网路岗 NAT 的实现并非依赖于 Windows 已有的内部功能,而是独立的。

网路岗 NAT 配置十分简单,大部分工作由系统自动探测完成。

在不影响上网速度的前提下,网路岗 NAT 能很好地对聊天软件和 P2P 下载软件进行过滤。在网路岗 NAT 基础上,用户能轻易实现多 Internet 出口的负载均衡功能,可以达到路由器的功能。

2. 安装网路岗 NAT

操作系统要求:Windows 2000/XP/2003。

安装说明:在安装网路岗软件时,NAT 并不被随带安装,当需要用到此功能时,可手动安装。在网路岗界面中选择"工具"→"安装服务"命令,弹出"安装服务程序"对话框,如图 8-18 所示。



图 8-18 "安装服务程序"对话框

在"服务类别"下接列表框中选择"共享上网服务(NAT)",单击"安装"按钮即可安装,安装完毕后需要重新启动网路岗 NAT 才能生效。

安装成功后,如果没有启用 DHCP 服务功能,则建议客户机将网关和 DNS 指向该安装 NAT 的机器。

重新启动机器后,在"高级设置"中单击"NAT 基本设置"选项,在弹出的 NAT 基本设置对话框(图 8-19)中进行简单设置。

(1) 选择本地网卡,也就是内网网卡。如果该网卡同时配置多个内部 IP,那么第一个 IP 地址及掩码所代表的网段就是能被共享的网段。

(2) 外网卡由系统自动探测,但必须保证该机器已能上网。

3. 网路岗 NAT 的过滤规则

在"高级设置"中单击"NAT 安全过滤"选项,在弹出的对话框中设置 NAT 过滤日期及时间安排和过滤项目。

(1) 过滤时间安排,如图 8-19 所示。

用户可根据需要设置过滤启用时间,该时间是针对所有过滤项目的总体控制。



图 8-19　NAT 基本设置

（2）过滤项目定义。以过滤 UDP 登录方式的 QQ 为例，在图 8-20 所示的“设置 NAT 过滤项目”选项组中选择 Tencent QQ（UDP mode）复选框，单击“添加”按钮，弹出“过滤项目”对话框，输入的起始端口号 8000 和结束端口号 80001 是针对每条通信的外网端口的，其他通信端口的过滤设置方式类似，如图 8-20 所示。



图 8-20　定义过滤端口

（3）黑名单。当系统检测到有机器恶意扫描外网端口时，系统自动将其归入黑名单，但并非无限期归入黑名单，当有效期过后，该机器又恢复正常。在 NAT 基本设置对话框中，单击“高级设置”按钮，弹出“高级设置”对话框，在该对话框中设置黑名单的封堵有效期。

8.3.2　常见系统配置

1. 网络定义

（1）定义内部网段，如图 8-5 所示。

只有出现多网段/多子网的情况，才需要定义内部网段。定义内部网段时，一般要求定义每个需要监控的 IP 段，也可采用简化的定义方式。例如，输入 192.168.0.1-192.168.1.255，这样只需要输入一次。

（2）设置代理 IP 或内网资源，如图 8-21 所示。



图 8-21　设置代理或内网资源

如果采用非透明代理服务器软件实现多机共享上网，必须在该处输入代理服务器的IP 地址(内网 IP 范畴)。另外，如果网内有邮件服务器等内网资源，也需要在该处输入其IP 地址，才能监控到内网机器访问内网资源的情况。

2. 监控项目(如图 8-22 所示)

常见网络活动监控项目
访问网站(HTTP)
发送邮件(SMTP))
接受邮件(POP3)
ICQ(英文聊天)
腾讯QQ(中文聊天)
异地上传或下载文件(FTP)
登陆异地电脑(TELNET)
文件访问与操作(NETBIOS)
Msn Messenger
Yahoo Messenger
启用Http标题缓冲
自定义项目...

图 8-22　监控项目

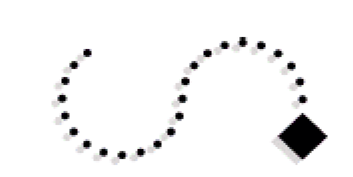
默认情况下，所有列出的项目都处于被监控状态，单击项目可以取消/选中该项目。

系统还提供了自定义项目，在定义项目时必须对 IP 通信有所了解，在监控项目对话框中单击“自定义项目”按钮，弹出“自定义监控项目”对话框，如图 8-23 所示。

项目定义
项目名称：
监控描述：
通讯类型：TCP　UDP
源 端 口：任意端口
目标端口：等于　0

图 8-23　自定义项目

“项目名称”文本框用以标识所定义的项目。



“监控描述”文本框中的内容将在“现场观察”窗口中显示并保存于对应的日志文件中。

“通讯类型”选项组中有 TCP 和 UDP 两个单选按钮，以后的版本中将增加其他通信类型。

“源端口”组合框用来输入或选择发出通信包的一方所占用的端口值。

“目标端口”组合框用来输入或选择接受通信方所使用的端口值。

如果系统检测到符合上述条件的通信包，将在“现场观察”窗口中显示出来，并记录到日志文件中。

3. 监控时间

监控时间对话框中显示的监控时间是全局的，在非监控时间段，监控服务完全不做任何控制，尽管服务还处于运行状态。

4. 端口配置

监控项目和端口是息息相关的，系统通过对特定端口数据的分析来实现对特定项目的监控。每一个项目可同时配置 3 个端口，例如，用户的网络有一天也许会同时出现 80、8080、3128 等访问网站的端口，这样就需要配置多个端口。

如果采用非透明代理服务器软件实现共享上网，且代理端口并非 80，那么就需要在 HTTP 的端口 80 后面再增加一个端口值。

5. 空闲 IP

通常，网络管理员在给网内机器分配完 IP 后仍有些 IP 范围段是空闲的，短期内用不上，而且网管也不想让这些 IP 被使用，那么，可以利用空闲 IP 防止计算机 IP 被私下更改就非常有效！

8.4　上网规则

1. 上网

“上网”选项卡如图 8-24 所示。

如果只是简单地控制目标机器的上网行为，在“上网”选项卡中设置是最好的。图 8-24 中蓝色显示块表示允许，白色显示块表示禁止。用鼠标指针来选择蓝色/白色显示块。

只有在白色时间段，对 Web 端口的封堵才起作用。在蓝色时间段是不是就一定可以上网还难说，主要看其他的选项卡中是否设置了封堵，在如此多的上网规则中，只要有一处封堵，就能起到封堵的作用。

如果用 Outlook 收发 hotmail 邮件，“上网”选项卡中的选项将不起作用，因为 hotmail 邮件并非通过收发邮件的端口(110/25)通信，而是通过 HTTP 方式通信。

2. 网页过滤

“网页过滤”选项卡如图 8-25 所示。

网页过滤主要是针对 URL 地址的过滤，对网页内容不予过滤。定义关键词的时候，建议输入最具代表性的词。

图 8-24 “上网”选项卡



图 8-25 “网页过滤”选项卡

对 google.com、baidu.com 和 3721 等搜索网站,还支持对中文关键词的封堵。

举例说明:

(1) 如果要禁止上 www.sina.com.cn 网站,则在“自定义禁止网站(包括搜索关键词)”组合框中输入 sina.com.cn 比较合适,如输入 sina.com,则被控机器连同 www.sina.com 和 www.sina.com.cn 都不能上了。

(2) 在“自定义禁止网站(包括搜索关键词)”组合框中输入“暴力”,以防被控机器在搜索网站上以该关键词来搜索。

(3) 在“只允许访问与工作学习有关的网站”组合框中输入 .sohu.只能上 www.sohu.com。

3. 过滤库

“过滤库”选项卡如图 8-26 所示。

为方便控制,网路岗软件专门收集了网站列表和端口库,可供用户选择。在如图 8-26 所示的“过滤库”选项卡中,单击“进入列表库管理工具”按钮,打开“DB 列表库管理中心”窗口,在该窗口中进行添加或删除操作。

列表库管理工具是专门针对网站列表库的工具,用户可以随意添加/删除/查询现有的列表库。如果有现成的列表文本文件,则可以导入到已打开的相应库中,被成功导入列表库的网站将被显示出来,通过导入与导出功能,用户之间可以轻松交流自己收集的网址。注意:不能查阅或导出系统固有的网站列表,这主要是出于知识产权方面的考虑。

4. 上网反馈

“上网反馈”选项卡如图 8-27 所示。

如果通过封堵端口的方式来禁止上网,则上述功能无效;必须通过关键词来封锁网站才有效。

在以前的网路岗软件版本中,封堵一台机器上某个网站时,会显示连接出错信息,因为默认设置为选中“反馈连接出错信息”单选按钮。为了让被封锁的机器显示更明确的信息,可以选中“反馈下列一段文字”单选按钮。



图 8-26　“过滤库”选项卡



图 8-27　“上网反馈”选项卡

另外，如果目标机器上了某个敏感网站，选中“转移到其他页面(URL)”单选按钮可以让其跳转到某一个指定的页面。

5. 邮件过滤

“邮件过滤”选项卡如图 8-28 所示。

邮件过滤并非严格过滤，这是因为如果邮件内容太少，甚至没有，那么系统检测到有邮件发送迹象时，该邮件可能已经发送出去，再去堵截就没有意义了。

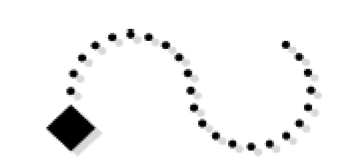
尽管如此，针对稍大的邮件的过滤还是有效的，尤其是带附件的邮件。

6. IP 过滤

“IP 过滤”选项卡如图 8-29 所示。

图 8-28　“邮件过滤”选项卡

图 8-29　“IP 过滤”选项卡



IP 过滤是针对因特网上各类资源的 IP 地址的过滤，进行 IP 过滤设置时，需要对 IP 有全面的了解。事实上，全球 IP 地址的分配是有一定规定的，相关知识可在网上搜索到，搜索关键词请用“IP 地址分配”，利用这些规定，可以设置某些地区的网站不可以上。

某些大型网站，例如，yahoo、sina 等都具有很多的 IP 地址，因此，不能简单地通过一两个 IP 地址来封锁该网站。

7. 封堵端口

“封堵端口”选项卡如图 8-30 所示。

封堵端口是略显专业化的功能名词，从网路岗一代开始就保留此功能，封堵端口功能是用户用得比较多的功能之一。

建立在 TCP/IP 通信之上的任何一款网络软件，都会用到端口，例如，股票软件、FTP 软件、收发邮件软件等，都具备自己的开放端口。因此，通过端口来封锁上网行为是非常有效的。

尽管很多软件的端口是软件开发者自定义的，但用户不必担心其改变自身的开放端口，因为，开放端口一旦改变，该软件的客户端也必须随之更改，从市场角度看是不现实的。

如果了解 IP 包，可利用本系统提供的 IP 包分析工具来分析端口。

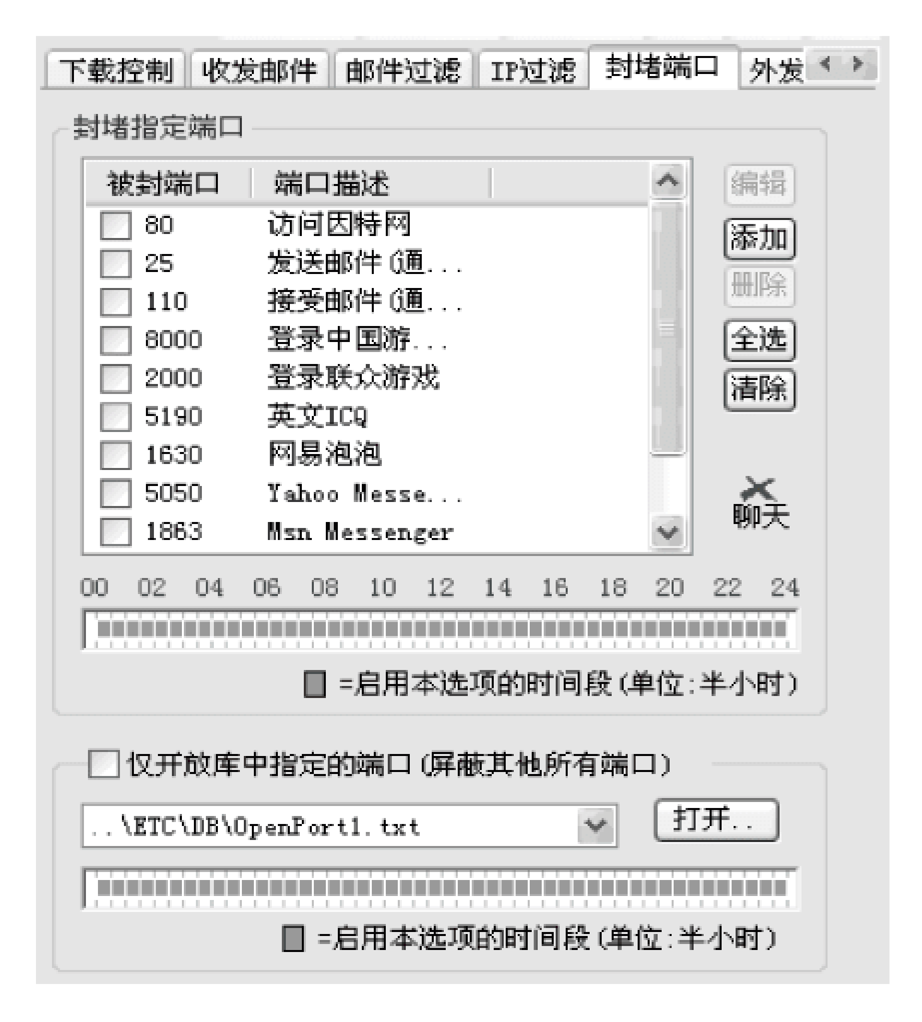


图 8-30 “封堵端口”选项卡

8. 外发尺寸

“外发尺寸”选项卡如图 8-31 所示。

对外发尺寸的控制是一种模糊控制，并不能精确到字节数，而且，只有在购买的版本具备邮件内容的监控功能时才起作用。如果没有内容监控功能，系统无法及时知道外发文件的大小，也就不能在中途进行堵截。

9. 限制流量

“限制流量”选项卡如图 8-32 所示。

首先说明，本软件只能检测到上网带宽数据而不能实现对带宽的管理和分配。尽管如此，根据客户的要求，该软件提供了对流量的限制功能。例如，限制某台机器每天只能有多少 MB 的上网流量，超过这个数字，系统会自动断网。

“限制流量”选项卡中显示的累计流量是动态的，便于及时观察到客户机的流量。

如果规定了该机器每分钟的流量，则每隔一分钟该机器累计流量就会自动变成 0。

10. 绑定 IP

“绑定 IP”选项卡如图 8-33 所示。

在单网段环境，且是基于网卡的网络监控模式下，可以通过绑定 IP 来防止目标机器私下更改 IP 上网。

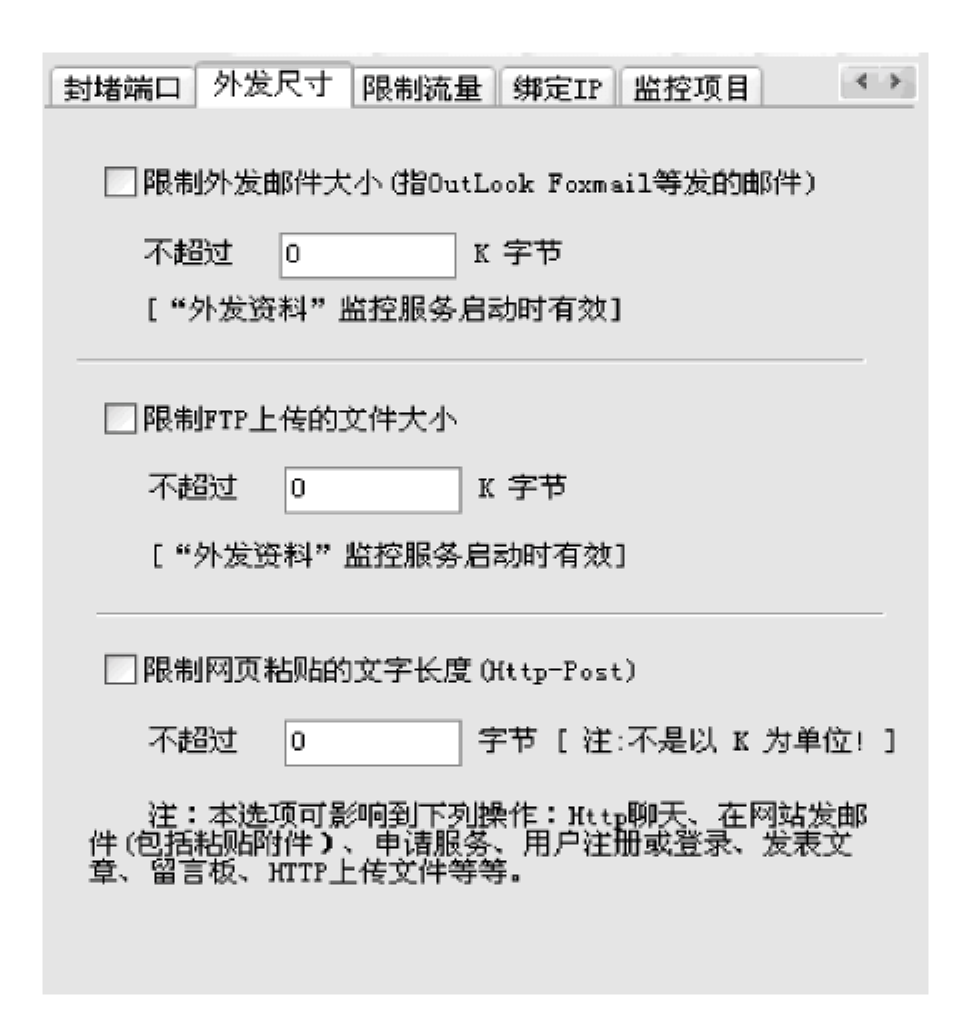


图 8-31 “外发尺寸”选项卡

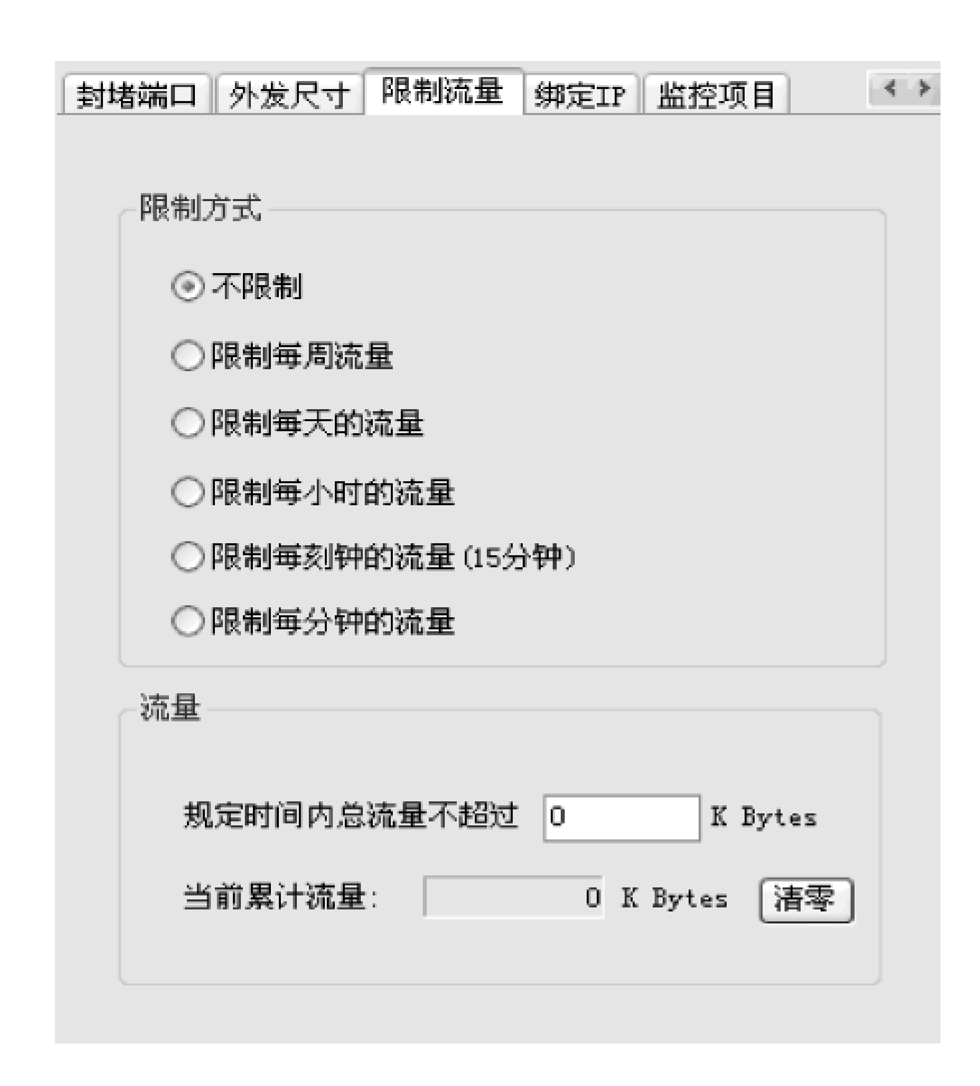


图 8-32 “限制流量”选项卡

在“绑定 IP”选项卡中选择“IP 改变时，记录其变化情况”复选框，则该网卡更改 IP 地址后，会详细记录其更改情况。

11. 功能项目

“功能项目”选项卡如图 8-34 所示。

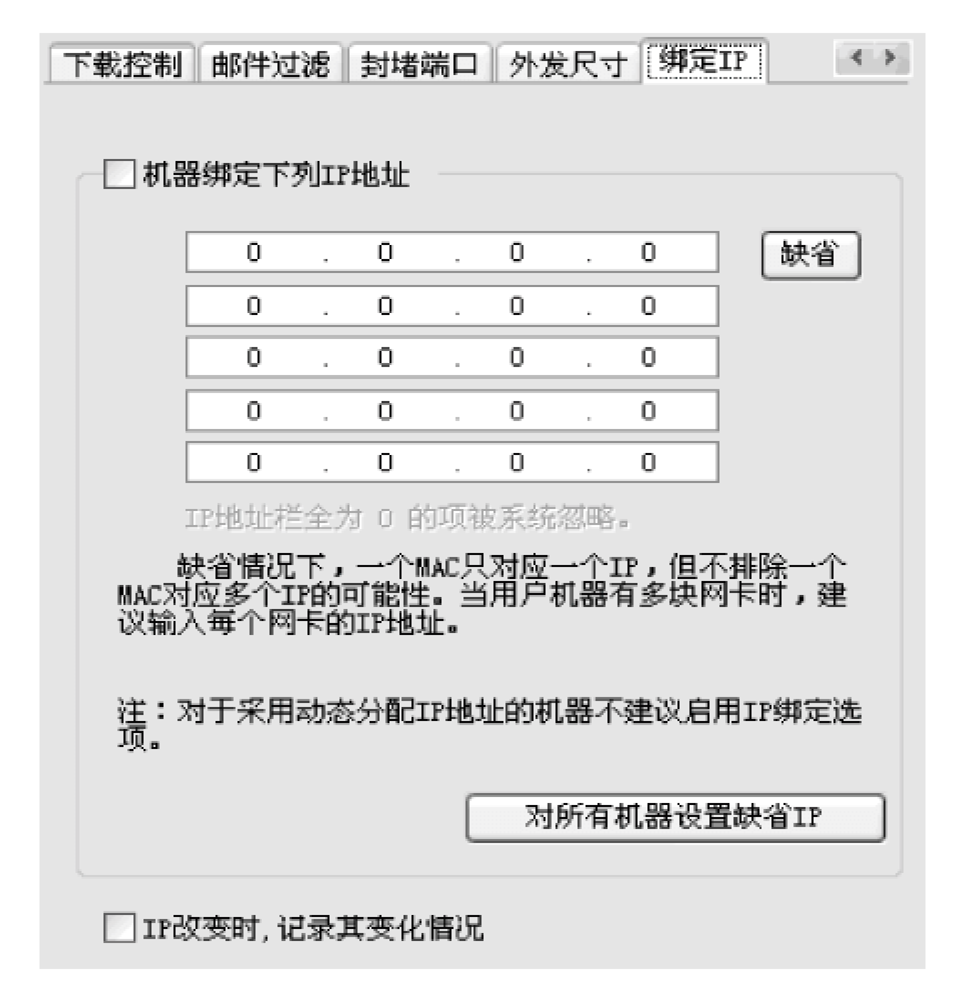


图 8-33 “绑定 IP”选项卡

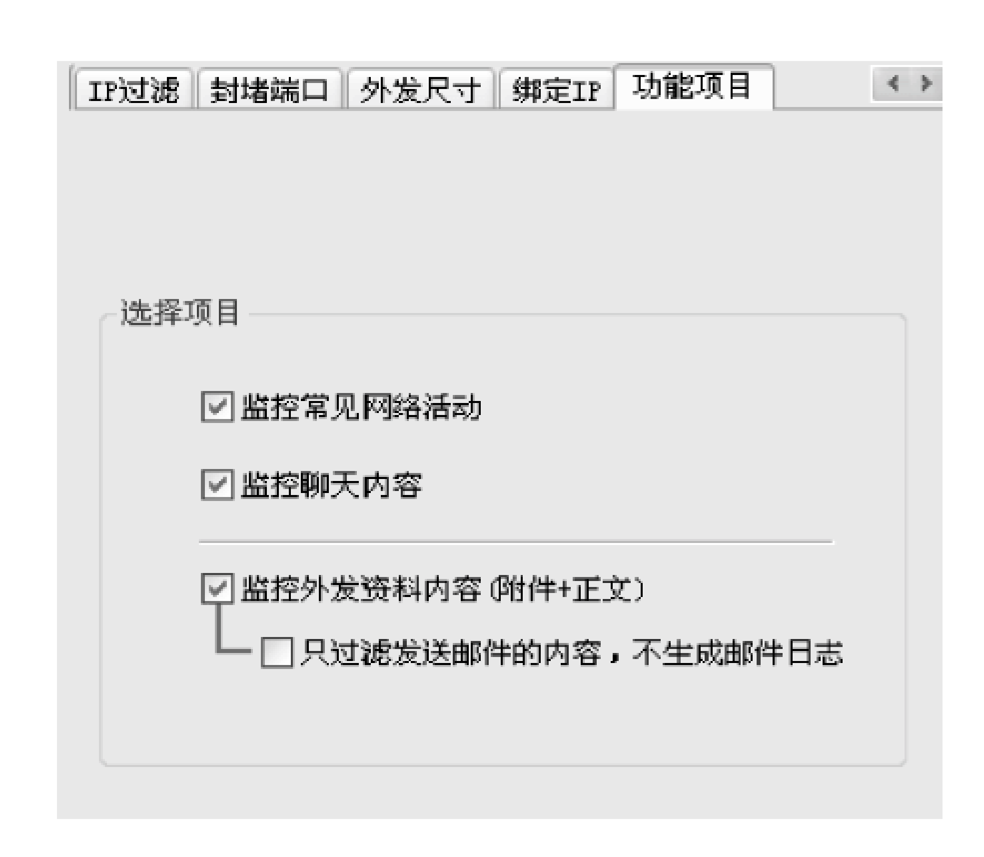


图 8-34 “功能项目”选项卡

在“功能项目”选项卡中可根据需要设置目标的监控内容。如果购买的版本没有邮件内容监控或没有聊天内容监控功能，则“监控聊天内容”和“监控外发资料内容(附件＋正文)”复选框就不起作用。如果只是想过滤邮件正文而不记录邮件，则可以选择“只过滤发送邮件的内容，不生成邮件日志”复选框。

8.5 日志查阅、日志报表及远程控制中心

8.5.1 日志查阅和日志报表

1. 查阅网络活动日志

（1）在网路岗界面工具栏中单击“网络活动”按钮，打开“查阅‘网络活动’日志”窗口，在该窗口中选择目标机器，如图 8-35 所示。

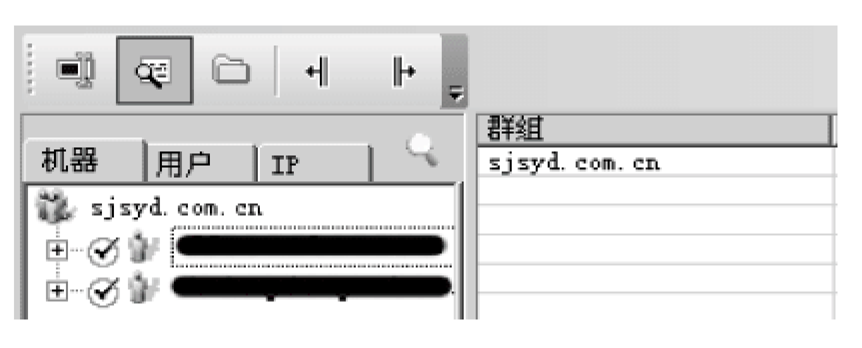


图 8-35 选择目标

选择“所有对象”，查询日志的时候，是针对所有机器的；相反，如果去掉所有对象前面的勾，可以随意双击某个目标机器，以显示该机器对应的日志记录，粗黑显示的机器表明有与其相关的日志记录。

图 8-35 中显示的“机器/用户/IP”是和选择的网络监控模式直接关联的，查阅日志的时候，请根据选择的网络监控模式来选择“机器/用户/IP”。

（2）统计日志

针对访问网站的日志和收发邮件的日志，网路岗软件提供了简单的统计功能。

2. 查阅外发资料日志

在网路岗界面工具栏中单击“外发邮件”按钮，打开“查阅‘外发资料’日志”窗口，在该窗口中选择目标机器，如图 8-36 所示。

图 8-36 显示的“机器/用户/IP”是和选择的网络监控模式直接关联的，查阅日志的时候，请根据选择的网络监控模式来选择机器/用户/IP 地址。

小图标表示是否存在附件。

小图标表示该邮件可直接用 Microsoft Outlook 打开。如果发现图 8-36 右下半部分显示乱码，建议用 Outlook 打开邮件。

单击小图标后可显示附件。

图 8-36 选择目标

8.5.2 远程控制中心

1. 授权

在使用远程日志查阅功能的时候，必须先在监控端进行授权。授权内容包括：用户名、登录密码、查阅日志的权限、授权查阅的范围等。在网路岗界面单击“远程客户机权限”选项，在弹出的对话框中单击“添加”按钮，弹出“远程客户机”对话框，如图 8-37 所示，在该对话框中进行授权设置。

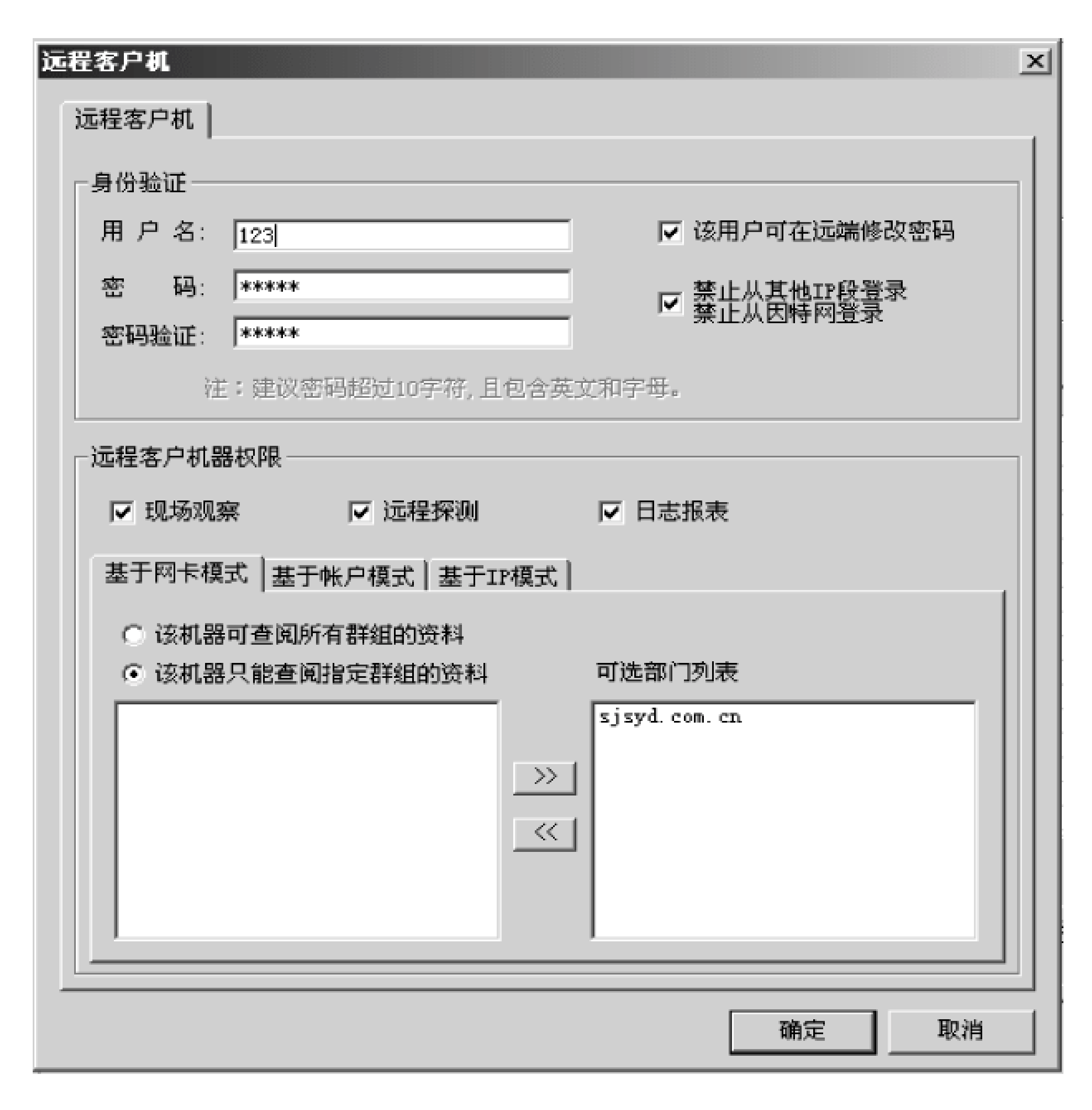


图 8-37　授权

2. 安装远程控制中心端程序

安装程序位于光盘中，安装后运行远程控制中心程序，弹出“远程控制中心”对话框，如图 8-38 所示。

数据交换口在监控机端有定义，默认是 9010 端口，如果希望更改数据交换端口，请在网路岗服务栏目项上双击打开如图 8-39 所示的对话框，修改数据交换端口后，重新启动数据交换服务。

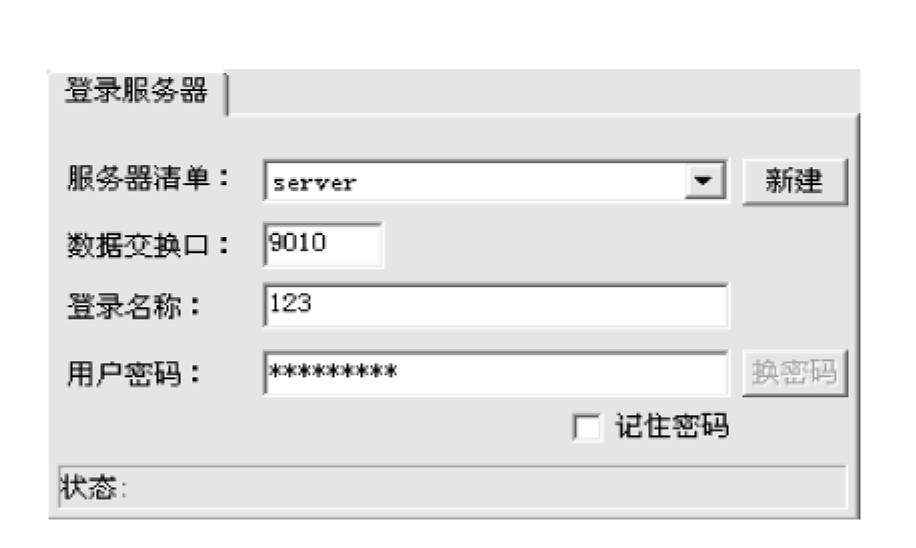


图 8-38　登录界面



图 8-39　安装设置

在输入用户名和密码后，登录服务器时可能碰到下面两个问题。

(1) 错误提示一："登录服务器失败"。

解决方法：

首先，检查服务器 IP 地址是否正确，如果没有问题，再用 Ping 命令检查。如果不能 Ping，则检查监控机上是否安装了个人防火墙软件，如有，则可能需要卸载再试。如果能够 Ping 监控机，则需要检查数据交换＜通信＞服务是否已经启动，而且两边的端口是否一致。

(2) 错误提示二："验证名和密码失败"。

解决方法：

检查监控机上授权的用户名和密码，如果检查不出任何问题，建议另外新建一个用户名再试。

3. 下载日志

一旦登录成功，可以通过菜单中的"下载日志"功能来选择下载日志内容。

8.6 本章小结

本章以网路岗为工具，介绍了网络管理软件的初步使用方法，并介绍了此款软件的安装、配置和使用过程。通过学习，要求掌握用网路岗软件进行简单网络管理的方法和使用技巧，并能触类旁通，使用其他简单网络管理软件对网络进行管理。

8.7 本章习题

参照本章所讲，在征得网络管理员同意的前提下，使用网路岗软件对所使用的网络进行管理。

第 1 步：安装网路岗软件；

第 2 步：绑定网卡；

第 3 步：监控模式设置为"基于网卡"模；

第 4 步：启动所有的后台监控服务；

第 5 步：检验是否安装正确；

第 6 步：封堵某台机器的 MSN 收、发邮件的端口，并检验封堵的效果；

第 7 步：查阅网络活动日志和外发资料日志。